VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH ZMĚN SYSTÉMU ŘÍZENÍ IDENTIT VE FIRMĚ

DRAFT OF CHANGES IDENTITY MANAGEMENT SYSTEM IN A FIRM

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. Vojtěch Vokálek
AUTHOR

VEDOUCÍ PRÁCE — Ing. Viktor Ondrák, Ph.D.
SUPERVISOR

BRNO 2016

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2015/2016
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Vokálek Vojtěch, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Návrh změn systému řízení identit ve firmě

v anglickém jazyce:

Draft of Changes Identity Management System in a Firm

Pokyny pro vypracování:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

BERTINO, E. a K. TAKAHASHI. Identity management: Concepts, Technologies, and Systems. Boston: Artech House, 2011. ISBN 978-1-608807-039-8.
ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006.
ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.
ITU. ITU-T Recommendation Y.2720 - NGN identity management framework. Geneva: International Telecommunication Union, 2009.
DOUCEK P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.
POŽÁR J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

Vedoucí diplomové práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2015/2016.

L.S.

_____	_____
doc. RNDr. Bedřich Půža, CSc.	doc. Ing. et Ing. Stanislav Škapa, Ph.D.
Ředitel ústavu	Děkan fakulty

V Brně, dne 29.2.2016

Abstrakt

Předmětem diplomové práce je prozkoumat integraci systému správy identit se systémem řízení bezpečnosti informací na základě teoretických poznatků a analýzy současného stavu. Upozornit společnost na nedostatky a podat návrhy na zlepšení.

Abstract

The subject of the Master thesis is to explore the integration of Identity Management System with the Information Security Management System based on theoretical knowledge and analysis of the current situation. Notify the company to gaps and make proposals for improvement.

Klíčová slova

Identity management, ISMS, bezpečnost, proces, společnost, role, architektura, přístup, cyklus, heslo

Keywords

Identity management, ISMS, security, process, company, role, architecture, access, cycle, password

Bibliografická citace

VOKÁLEK, V. *Návrh změn systému řízení identit ve firmě.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 71 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D..

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně.

Prohlašuji, že citace použitých pramenů je úplná, že jsem v práci neporušil autorská práva (ve smyslu zákona č. 121/2000 Sb. o právu autorském a o právech souvisejících s právem autorským).

V Brně, dne 25. května 2016

. . . . . .

podpis autora

Poděkování

Děkuji panu Ing. Viktorovi Ondrákovi, Ph.D. za profesionální přístup při vedení práce. Dále děkuji zaměstnanci ze společnosti XYZ za poskytnuté informace.

Obsah

ÚVOD

V dnešním světě vysoké konkurence, jsou investice společností do informačních technologií klíčové pro podporu jejich byznysu. Pokud chce společnost minimalizovat náklady, musí tyto technologie efektivně využívat. Musí se také umět vypořádat s výskytem nových zranitelností, hrozeb a rizik, kterými jsou informační aktiva společnosti vystaveny. Jedním z prostředků, které přispívají k vyšší bezpečnosti aktiv je systém řízení identit.

Organizace se v průběhu času rozrůstají. Roste množství softwarových aplikací a zaměstnanců. Zaměstnanci obdrží uživatelské jméno a heslo, aby se k aplikaci mohli přihlásit. V žádném případě nemůže existovat svobodný přístup k aktivům společnosti. S přibývajícím počtem aplikací roste počet žádostí o uživatelská jména, což klade nároky na paměť uživatele. Do aplikací potřebují přístupy nejen zaměstnanci firmy, ale i dodavatelé a další partneři. Nedisponuje-li společnost žádným systémem řízení identit, správa je mnohem složitější a nákladnější. Uživatelé si musí identity do systémů pamatovat. Správci musí přístupová práva pro všechny systému nastavovat ručně. Tyto aspekty vedou k větší pravděpodobnosti chyb lidského faktoru. Hrozí, že bude narušena bezpečnost aktiv společnosti. Řízení identity může výše zmíněné problémy vyřešit. Myšlenka identity management je centralizovat správu identit a přístupu. Místo toho, aby aplikace měli své vlastní autentizační a autorizační mechanismy, správa je centralizovaná.

V diplomové práci budu zkoumat integraci identity managementu ve společnosti XYZ se systémem řízení bezpečnosti informací (ISMS). Společnost přepracovala nutné procesy pro certifikaci ISO/IEC 27001, ale k detailnímu zmapování IdM procesu nedošlo. Je zde pravděpodobnost bezpečnostních trhlin, které je v případě nalezení nutné odstranit. IdM proces byl převzat z globální úrovně a upraven pro potřeby lokální pobočky.

CÍL A METODIKA

Cílem práce je vypracovat soubor návrhů a doporučení systému řízení identit tak, aby se zlepšily již zaběhnuté procesy a posílila bezpečnost. IdM zavedený ve společnosti XYZ musí korespondovat s požadavky ISO/IEC 27001 a norma se musí dodržovat. Hlavním požadavkem společnosti je mít jistotu, že v IdM procesu nejsou žádné bezpečnostní trhliny, které by narušily bezpečnost a reputaci u zákazníků. K dosažení cíle použiji doporučení z rodiny norem ISO/IEC 27000 a rámec systému pro řízení identit. Samozřejmostí je také analýza současného stavu a další prvky teoretických východisek.

1 TEORETICKÁ VÝCHODISKA

Teoretická část se věnuje problematice ISMS a identity managementu.

1.1 Základní pojmy

Aktivum

Vše, co má pro organizaci hodnotu.

Hrozba

Hrozba (Threat) je pojem používaný v řízení rizik. Je to událost, která ohrožuje bezpečnost.

Riziko

Označuje nejistý výsledek s možným nežádoucím stavem. Kombinuje hrozbu a zranitelnost s dopadem na aktivum.

Událost

Identifikovatelný stav systému, služby nebo sítě s možným porušením bezpečnostní politiky.

Incident

Je neočekávaná událost, u které je velká pravděpodobnost, že bude narušena bezpečnost informací.

Identifikace

Proces určení identity subjektu v databázi záznamů. Například pomocí otisků prstů.

Autentizace

Proces ověření identity subjektu s požadovanou mírou záruk přístupu do systémů. Například pomocí hesla.

Autorizace

Je proces získání souhlasu k provedení aktivity. V případě IdM systému slouží jako ochrana proti zneužití.

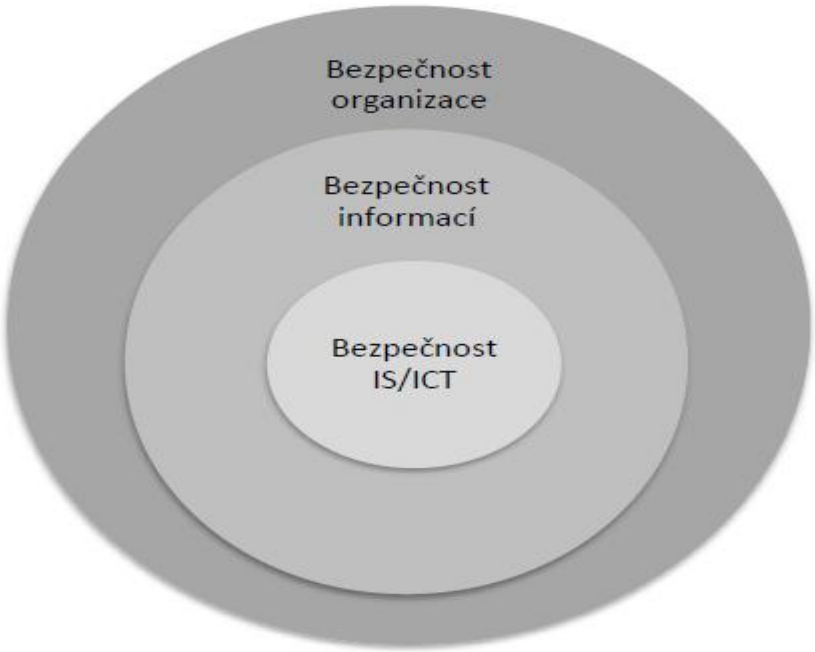
Next Generation Network (NGN)

Sítě nové generace vznikly sloučením datových a telefonních sítí. Jejím cílem je poskytovat komplexní síťové služby založených na IP. Jedná se o síť s vysokou propustností. Výhodou NGN sítí je vytvoření jednotné komunikační sítě, čímž se snižují náklady na provoz a správu sítě. Příkladem je VoiP telefonie [1, 5].

1.2 Systémy řízení bezpečnosti informací

V dnešní době jsou informace velice cenným artiklem. Společnosti si musí uvědomit, že s nimi spojené systémy, procesy a lidské zdroje jsou aktiva k dosažení cílů organizace. Omezení jejich dostupnosti, ztráta důvěrnosti a integrity, může mít nepříznivý dopad na fungování celé organizace. Proto ochrana informačních aktiv je základním předpokladem pro dosažení stanovených cílů [4].

Bezpečnost informací se zabývá ochranou a dostupností. Řeší tedy přístupy a chrání je proti zneužití. Nejedná se pouze o informace v digitální podobě, ale o všechny typy informací. Bezpečnost informací je ve vzájemném vztahu s bezpečností IS/ICT a bezpečností organizace. Bezpečnost IS/ICT se stará o ochranu informačního systému a komunikačních technologií. Bezpečnost organizace chrání majetek. Na obrázku je vidět celé schéma [1]:



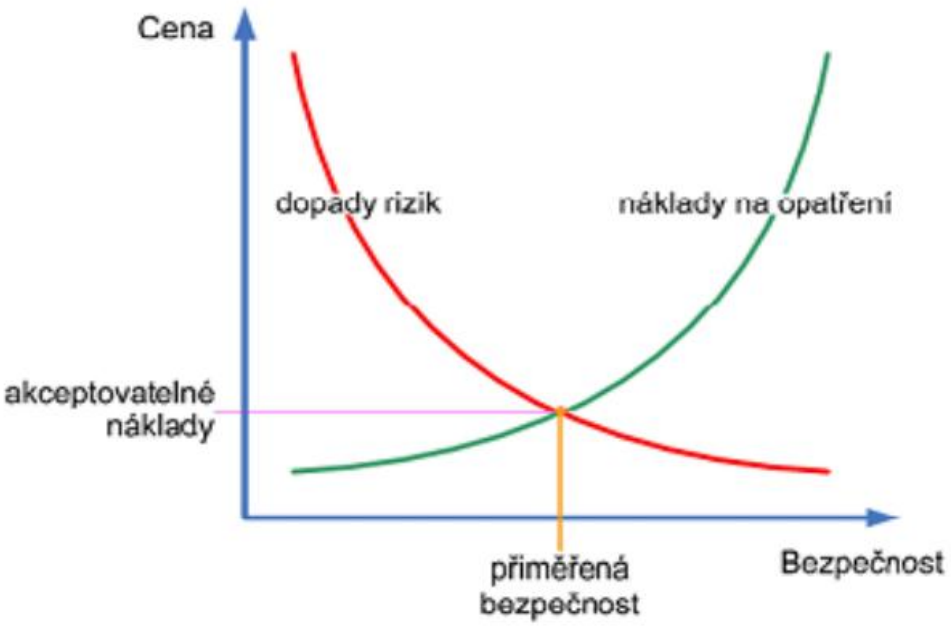
Obr.č. 1: Vzájemné vztahy bezpečností v organizaci

Zdroj: Upraveno dle [1]

S neustálými změnami uvnitř organizace vznikají nová rizika, která je nutné identifikovat a ošetřit. Je potřeba zlepšovat příslušná opatření nebo zavádět nová. Aby všechny činnosti byly ve vzájemných vztazích, měla by každá společnost stanovit politiku a cíle. Těchto lze cílů dosáhnout pomocí řídícího systému ISMS, který zavádí rodina norem ISO 27000 [4].

1.3 ISMS

*„ISMS je efektivní dokumentovaný systém řízení a správy informačních aktiv s cílem eliminovat jejich možnou ztrátu nebo poškození tím, že jsou určena aktiva, která se mají chránit, jsou zvolena a řízena možná rizika bezpečnosti informací, jsou zavedena opatření s požadovanou úrovní záruk a ta jsou kontrolována.“[*2]. Jeho úkolem je zavést pravidla a postupy řízení bezpečnosti informací v organizaci. Může být však zaveden pro dílčí část jako je informační systém, organizační složku, atd. Pro efektivní implementaci je důležitá informační aktiva analyzovat a použít vhodná opatření. Bezpečnost aktiv nikdy nemůže dosáhnout sta procent. Investice do zabezpečení by měla být na akceptovatelné úrovni nákladů. Hledá se tedy přiměřená bezpečnost za akceptovatelnou cenu [1, 3].



Graf č. 1: Graf přiměřené bezpečnosti za akceptovatelné náklady

Zdroj: [1]

1.4 Normy ISMS

Zavádění ISMS se řídí podle platných norem, které jsou mezi sebou provázané. Obsahují různá doporučení a směrnice. Mají za úkol organizacím pomoci se zavedením ISMS.

ČSN ISO/IEC 27000 – Přehled a slovník

Norma poskytuje přehled systému řízení bezpečnosti informací. Definuje pojmy a terminologický slovník pro ostatní normy z rodiny ISMS. V současnosti je platná norma z roku 2014 [1].

ČSN ISO/IEC 27001 – Požadavky

Tato mezinárodní norma specifikuje požadavky na zřízení, zavedení, provozování, monitorování, udržování a zlepšování systému řízení bezpečnosti informací, (Information Security Management Systems nebo ISMS). Jsou zde stanoveny cíle opatření, která jsou propojeny s těmi v normě ISO/IEC 27002. Norma slouží nejen certifikačním orgánům, ale i interním a externím subjektům. V současnosti je platná norma z roku 2013 [1, 6].

ČSN ISO/IEC 27002 – Soubor Postupů

Norma poskytuje doporučení a obecné principy pro řízení systému bezpečnosti informací v organizaci. Doporučení poskytují organizaci podporu při dosahování její cílů. Podle normy může organizace vyvíjet své bezpečnostní standardy a umožňuje velmi rychle zjistit stav bezpečnosti informačního systému. V současnosti je platná norma z roku 2013 [1, 7].

ČSN ISO/IEC 27006 – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

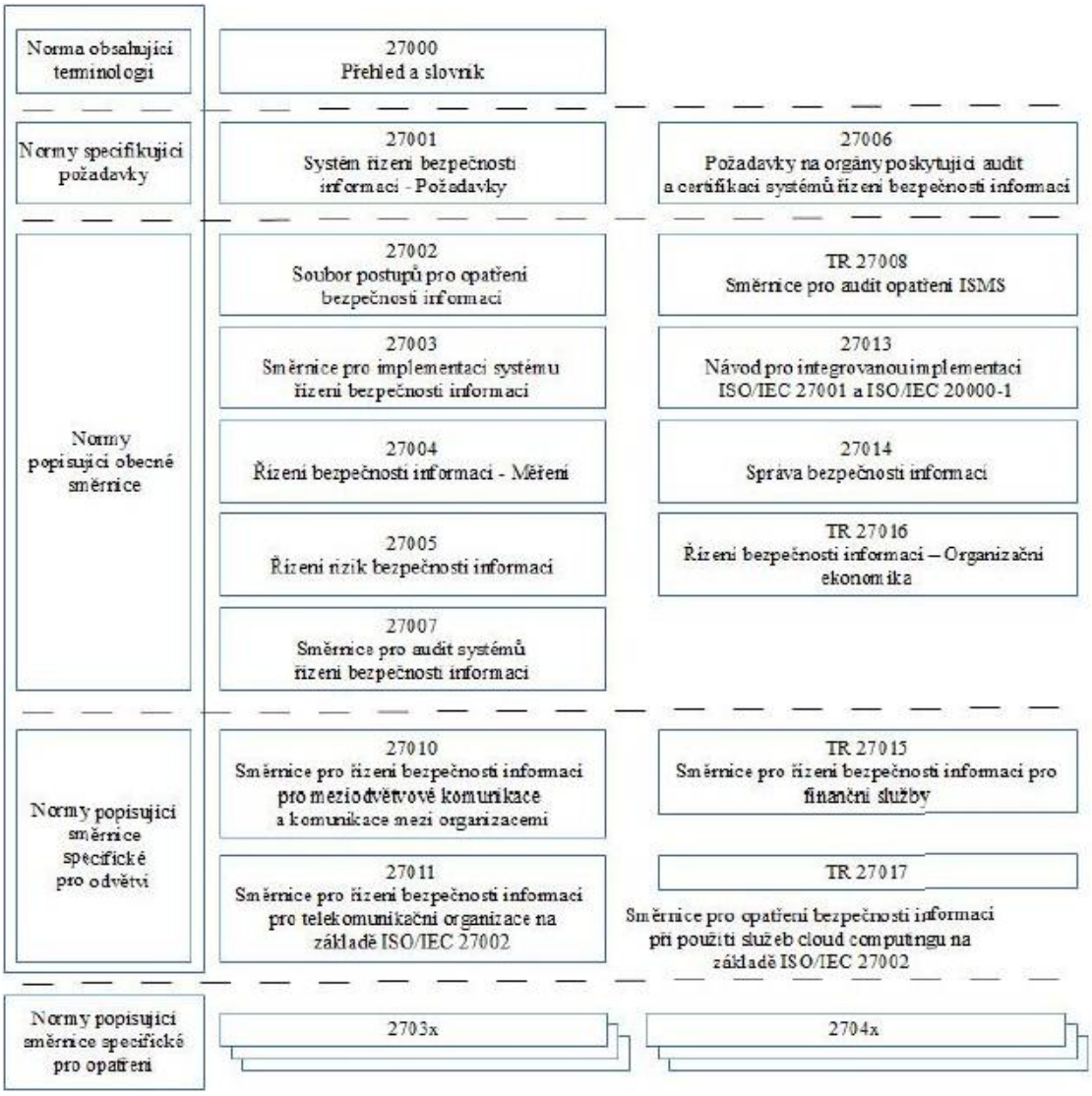
Norma specifikuje požadavky a poskytuje doporučení pro orgány provádějící audit a certifikaci řízení bezpečnosti informací. Norma podporuje proces pro akreditace pro tyto orgány. V současnosti je platná norma z roku 2011 [1, 5].

ČSN ISO/IEC 27007 – Směrnice pro audit systémů řízení bezpečnosti informací

Norma obsahuje doporučení pro řízení auditů ISMS, pro provádění auditů a pro odbornou způsobilost auditorů. Čerpá z normy ČSN EN ISO/IEC 19011, což je směrnice pro auditování systému managementu jakosti nebo environmentálního managementu. V současnosti je platná norma z roku 2011 [1, 5].

ČSN ISO/IEC 27008 - Směrnice pro kontrolu auditu systémů řízení bezpečnosti informací

V normě jsou doporučení auditorům ISMS, doplňuje normu ISO 27007 V současnosti je platná norma z roku 2011 [1, 5].



Obr.č. 2: Vztahy mezi normami řady ISMS

Zdroj: Upraveno dle [5]

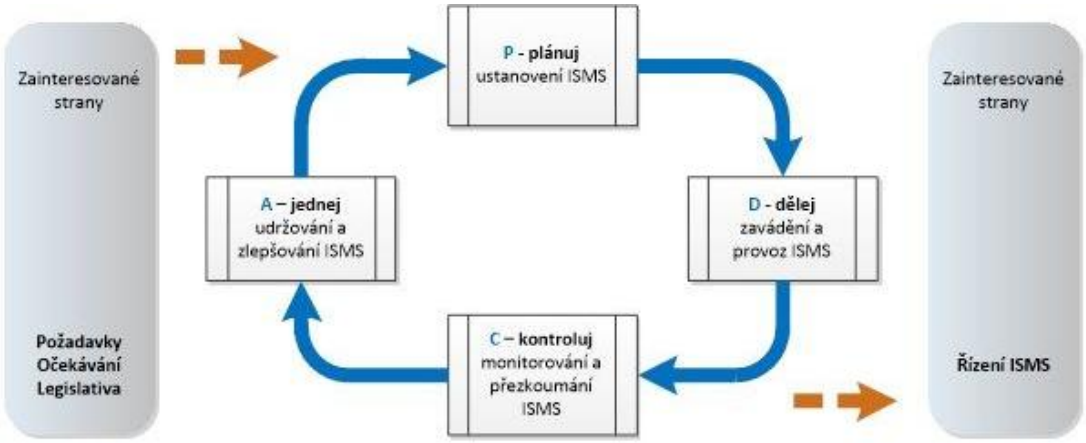
1.5 Model PDCA

Procesní přístup používaný v ISMS se nazývá Demingův cyklus (PDCA). Vynalezl jej E. Dwards Deming. Po druhé světové válce se účastnil plánování sčítání japonského lidu. Jeho zkušenosti v oblasti statistické kontroly kvality ho kvalifikovali do Japonské unie vědců a inženýrů. Postupně předal své know-how stovce japonských inženýrů, manažerů a studentů v oblasti řízení kvality a statistické kontrole procesů. Kombinace vysoké kvality se snižováním nákladů skutečně dovedla japonské společnosti k úspěchu. Model je použit v mnoha mezinárodních normách. Lze jej aplikovat nejen

pro celý systém managementu služeb, ale i pro jednotlivé části životního cyklu služby [1].

Používá se ke strukturovaným řešením problémů. Je to metoda postupného zlepšování například kvality, výrobků, služeb, aplikací, procesů či dat probíhající v cyklu čtyř činností:

- **Plan**: Analýza plánu
- **Do**: Implementace plánu
- **Check**: Monitorování a přezkoumání výsledku oproti původnímu záměru
- **Act**: Ponaučení se z chyb a na jejich základě přijmout opatření k nápravě a neustálému zlepšování



Obr.č. 3: Model PDCA v ISMS

Zdroj: [4]

1.5.1 Ustanovení

Fáze ustanovení ISMS je klíčovou částí budování ISMS, jelikož definuje základy celého systému řízení bezpečnosti informací. Pokud etapa není provedena s patřičnou důkladností, výsledky se promítají do dalších fází, což může nepříznivě ovlivnit celý systém. Je proto důležité naplánovat všechny souvislosti již v první etapě. Mnoho organizací není dostatečně připraveno na budování ISMS a pokud si své chyby uvědomí v dalších etapách životního cyklu, jsou finanční náklady na změnu větší. Pozdější provedení změn vyžaduje větší úsilí [2].

Je tedy nutné provést a zdokumentovat následující činnosti.

- Definovat rozsah a hranice ISMS
- Prohlášení o politice ISMS
- Definovat a popsat přístup k hodnocení rizik
- Identifikovat rizika a ohodnotit aktiva
- Analyzovat a vyhodnotit rizika
- Identifikace variant pro zvládání rizik
- Výběr bezpečnostních opatření
- Souhlas vedení organizace k provozování ISMS
- Prohlášení o aplikovatelnosti

Prvním krokem plánování systému řízení informační bezpečnosti je potřeba vedení přesvědčit o všech výhodách, podpořenými doporučeními, jenž jsou uvedeny v normě ISO 27002. Vytvořit obchodní případ zavedení ISMS a vysvětlit analýzu rizik. Dokument popisující rozsah ISMS ukazuje, jaké části budou systémem řízení informační bezpečnosti pokryty. Jedná se například o systémy, oddělení, atp. Dále je definován systematický přístup k ohodnocení rizik. Je vybrána vhodná metodika například CRAMM a kritéria pro akceptaci rizika. V identifikaci aktiv jsou popsána aktiva, která jsou určena k identifikaci a hodnocení ve formě tabulky. Dokument slouží pro vytvoření seznamu sítí, databází, datových entit, atd. Zpravidla bývá uložen v konfigurační databázi. Tento seznam je vstupem pro identifikaci rizik. Výstupem jsou konkrétní výsledky identifikace rizik. Jsou aplikována bezpečnostní opatření pro minimalizaci rizik. Některá rizika je třeba akceptovat, jelikož neexistuje způsob, jak je minimalizovat. Dalším dokumentem je tedy popis akceptace rizik. Poledním krokem je formální souhlas vedení organizace se zbytkovými riziky. Následně je vydáno prohlášení o aplikovatelnosti popisující cíle bezpečnostních opatření [1, 4].

1.5.2 Zavádění a provoz

Druhá fáze se zaměřuje na implementace bezpečnostních opatření z druhé etapy. Podstatné je připravit dílčí plány projektu, upřesnit termíny, určit zodpovědné osoby, atd. Mělo by dojít k vysvětlení principů manažerům a uživatelům [2].

Je nutné realizovat tyto činnosti:

- Stanovit základní dokument pro zvládání rizik

- Implementovat plán zvládání rizik a aplikovat postupy opatření v definovaných oblastech
- Určit způsoby, jak opatření měřit a sledovat vybrané ukazatele
- Zavézt program budování bezpečnostního povědomí uživatelů
- Zavézt postupy pro rychlou detekci bezpečnostních incidentů
- Řídit provoz ISMS

Vytvoření implementačního plánu ISMS navazuje na prohlášení o aplikovatelnosti z předchozí etapy a plánu zvládání rizik, který je převeden do praxe. Při provádění opatření se musí brát ohled na finanční situaci organizace a dodržovat pravidlo akceptovatelných nákladů. Vzhledem ke komplexnosti ISMS je obecně žádoucí při implementaci dle ISO 27002 rozdělit projekt na dílčí projekty. Výstupem fáze je zavedení ISMS, vytvoření procedur pro interní audit, definice metrik, procedury zabezpečující vhodné řízení provozu ISMS, dokumentace řízení zdrojů. Dále pak vytvoření seznamu nápravných opatření pro zjištěná rizika včetně seznamu preventivních opatření. Vlastní nasazení a spuštění systému řízení informační bezpečnosti včetně všech činností není jednorázová aktivita, je nutné zavést proto proces neustálého vyhodnocování aktivit. Nedílnou součástí je budování bezpečnostního povědomí, jehož cílem je, aby zaměstnanci odborně působily ve výkonu činností. Je potřeba zaměstnance školit a umožnit jim profesní růst. Nutné je zavést postupy a obstarat nástroje pro detekci bezpečnostních incidentů a získané výsledky a zkušenosti využit k optimalizaci ISMS [2, 4].

1.5.3 Monitorování a přezkoumání

Ve třetí etapě Demingova cyklu je třeba prověřit zavedené bezpečnostní opatření a zajistit účinné zpětné vazby. Začíná se u kontroly osob jejich nadřízeným a fungování ISMS pomocí interních auditů. Cílem etapy je za pomoci zpětných vazeb připravit podklady pro vedení organizace o skutečném fungování ISMS, které je potřeba přezkoumat, zda korespondují s obecnými potřebami organizace. Přezkoumání probíhá alespoň jedenkrát ročně. [2].

Je potřeba provést následující činnosti:

- Ověřit účinnost bezpečnostních opatření

- Povést interní audity ISMS
- Vytvořit zprávu o celkovém stavu ISMS a jejím základě přehodnotit ISMS na úrovni vedení organizace

Aby bylo možné vyhodnotit shody s požadavky při zavedení ISMS, je nutné systém monitorovat a kontrolovat. Na základě získaných podkladů, doporučení a politik jsou informace vyhodnoceny a zpracovány. Pak je možné provést audit interními nebo externími auditory. S ohledem na změny v organizaci nebo v legislativě jsou přehodnocena zbytková a akceptovatelná rizika. Evidují se činnosti, které mohou mít dopad na ISMS. Sledování systémových logů, záznamy firewallu, protokolů detekce narušení, a dalších mechanismů. Provádí se první úroveň certifikace neboli předcertifikační ohodnocení. To poskytuje nezávislý pohled na provoz ISMS. Certifikační audit má ověřit, jestli systém řízení bezpečnosti informací koresponduje s požadavky ISO 27001. Pokud jsou zjištěny nedostatky, jsou odstraněny ve fázi udržování a zlepšování ISMS [2, 4].

1.5.4 Udržování a zlepšování

Poslední etapou celého cyklu je udržování a zlepšování ISMS. Cíl je zlepšovat, zavádět, kontrolovat a zpětně vyhodnocovat nápravná opatření. K tomu jsou potřeba informace z auditů a činností společnosti [2].

Je potřeba provést následující činnosti:

- Zavést zlepšení ISMS a dosáhnout požadovaných cílů
- Provést odpovídající preventivní a nápravné činnosti pro správnou funkci ISMS

Proces udržování a zlepšování slouží k sladění mezi obchodními požadavky, riziky a možnostmi informační bezpečnosti. Spolu se systémy řízení kvality společnosti přináší systematické řízení procesů ISMS. Smyslem při odstranění nedostatků je poučit se a předejít tak jejich opakování [4].

1.6 Identita

Než bude rozebrána problematika identity managementu je potřeba objasnit pojem identita a souvislosti s ní spojené. Existuje několik definic identity. Například:

„identitu jednotlivé osoby může obsahovat mnoho dílčích identit, z nichž každá představuje osobu v určitém kontextu nebo roli. Dílčí identita je podmnožina atributů hodnot kompletní identity, kde kompletní identita je sjednocení všech hodnot atributů ze všech totožností této osoby“ [13].

Tato definice se vztahuje pouze na osoby jako subjekty identit. Většina lidí si pod pojmem identita představí právě lidskou bytost. Identitu lze však chápat i jako neživé předměty. Identitu může představovat software a hardwarová zařízení. Nehledě na to, že v dnešním světě se stává výpočetní technika všudypřítomnou a identitám se běžně přiřazují objekty jako zboží, budovy, atd. Ty lze monitorovat a sledovat pomocí senzorů. Tato práce se zaměřuje na identity jako osoby. Obecně lze identitu chápat jako reprezentace entity v určité aplikační doméně. Například registrované osobní údaje zákazníka banky, případně i fyzické vlastnosti zákazníka tvoří identitu v rámci domény této banky. Identity obvykle souvisí s reálnými subjekty. Typicky reálnými identitami jsou lidé nebo organizace. Předpokladem je, že jedna identita nemůže být sdílena s více než jednou entitou. Mohou ale existovat sdílené entity. Například rodina tvoří identitu a odpovídá více členům. Nicméně, pokud jde o poskytovatele služeb, ti se zabývají reálnou entitou (rodinou), ale ne jejich členy. Osoba nebo organizace může mít nulu nebo více identit v rámci jedné domény. Například osoba může mít dvě identity ve školním systému, protože působí jako rodič a učitel ve škole. V systémech jsou nastavena pravidla pro registraci identity. V rámci domény určují, zda je povoleno více identit pro jedenu entitu. Pokud se i přes zákaz v systému registrace pro více identit objeví, jedná se s největší pravděpodobností o omyl nebo podvod. Jedna osoba může mít samozřejmě různé identity v různých doménách. Například osoba může mít jednu identitu spojenou jako zákazník v bance a další identitu jako pracovník v podniku. Identity se skládají z atributů a identifikátorů. Atributy mohou a nemusí být unikátní v rámci domény identity. Mají různé vlastnosti. Mohou být například přechodné, trvalé, vybrané automaticky nebo vydané příslušným orgánem. Atributy identit se mohou lišit v závislosti na typu entity. Například datum narození platí pro lidi, ale ne pro organizace [1, 9].

Podle doporučení ITU-T Y.2720 se identita skládá z identifikátorů (identifiers), ověřovacích údajů (credentials) a atributů (attributes) [14].

- **Identifikátory** - Jsou číslice, znaky a symboly, nebo jakékoliv jiné formy údajů sloužící k identifikaci subjektu v daném čase a místě. Například uživatelská jména účtu, číslo občanského průkazu, mobilní telefonní číslo a čísla zaměstnanců.

- **Ověřovací údaje** – Nebo také autentizační údaje jsou soubory údajů, které poskytují důkazy o pravosti identity. Ověřovací údaj může být generován na základě jednoho nebo více ověření. Můžou to být hesla, digitální certifikáty, biometrické informace a tikety.

- **Atributy** - Jsou data, která popisují vlastnosti subjektu. Údaje zahrnují základní informace využitelné k identifikaci (např. jméno, bydliště a datum narození, věk, pohlaví, role, záznamy) nebo informace generované v důsledku činnosti subjektu.

Ověřovací údaje a atributy mají další rozdělení.

1.6.1 Ověřovací údaje

Ověřovací údaje mají dvě základní vlastnosti. Integritu a validitu. Integrita říká, že s obsahem nebylo nijak manipulováno. Toho lze docílit použitím digitálního podpisu. Validita je složitější, aby byly ověřovací údaje prohlášeny za validní, musí projít procesem ověření. Ověřovací procesy se mohou lišit v závislosti od poskytovatelů identit. Na základě výše zmíněných vlastností lze ověřovací údaje klasifikovat [8].

- **Validní** - Digitálně podepsané po validaci.

- **Autentizované** - Digitálně podepsané, ale nevalidované.

- **Surové** - Digitálně podepsané sama sebou a nevalidované.

Ověřovací údaje se dále dělí na fyzické a digitální. Vývojem technologií vnikají jejich elektronické varianty. Například pasy obsahují čipy a dokážou komunikovat s výpočetní technikou. Digitální ověřovací údaj je například certifikát. Na základě výše zmíněných typů a vlastností se dají rozdělit [8].

- **Primární** - Zde patří významné životní události. Například narození, sňatek, promoce nebo smrti.

- **Sekundární** - Člověk prokazuje, že je tím, za koho se vydává. Jejich platnost závisí na zdrojových dokumentech. Sekundární ověřovací údaje identity obsahují identifikační fotografie a biometrické informace.

- **Terciální** - Patří sem členské karty, zaměstnanecké odznaky, apod. Jsou vydávány na určitou dobu a mají omezený účel.

1.6.2 Atributy

Atributy identity jsou digitální záznamy a používají pro transakce nebo jiné účely. Je zde velké množství možných identit atributů. Lze je rozdělit následujícím způsobem [8].

- **Právní dokumenty** - Slouží k jednoznačné identifikaci subjektu. Například čísla pasů, fiskální kódy, čísla sociálního zabezpečení. Dokumenty s nimi spojené jsou považovány za nejsilnější doklady totožnosti a měly by být silně zabezpečeny.

- **Demografické** - Tyto atributy typicky obsahují informace jako věk, pohlaví, země pobytu a adresu bydliště. Na jejich základě nelze subjekty jednoznačně identifikovat. Kombinací s jinými informacemi však k identifikaci dojít může.

- **Finanční** - Obvykle úzce souvisí s finančními institucemi. Zahrnují kreditní karty a čísla bankovních účtů. Takové atributy jsou častým terčem zlodějů. Je potřeba je silně chránit.

- **Biometrické** - Tyto atributy obsahují různé fyzikální vlastnosti subjektů. Představují důležité prostředky k ověření identity subjektů. Například otisky prstů, podpis nebo sken duhovky.

- **Transakční** - Jsou velmi dynamické. Atributy obsahují informace o pohybu a práci v internetu. Jde o různé zákaznické preference produktů a služeb.

1.6.3 Kategorizace identit

Identity lze kategorizovat mnoha způsoby z různých perspektiv. Zahrnují širokou škálu oborů včetně sociologie, psychologie, filozofie a počítačové vědy. První rozdělení identit je podle zúčastněných stran [8].

- **Jednotlivci** - Pro jednotlivce jsou identity nezbytné pro užívání personalizovaných služeb, sociálních sítí, blogů a virtuálních světů. Webové služby jsou nevyhnutelně založeny na identitách, protože to je nemožné komunikovat nebo se socializovat bez identifikace cílových stran.

- **Podnikové** - Přístup k informačním technologiím má dnes takřka každý. Společnosti si uvědomují obrovské příležitosti, které nabízí využívání identifikačních údajů. Například cílové reklamy a servisní služby. Kromě toho podniky mají zájem o efektivní správu identit, která bude v diplomové práci řešena.

- **Vládní** - Vlády hrají role poskytovatelů služeb identit a tvůrce politik. Mnoho vlád pracuje na digitálních projektech identit pro občany a zaměstnance. Například centrální registry občanů. Cílem je cílem přispět k rozvoji internetové ekonomiky, posílit důvěru a bezpečnost.

Identity jsou nejvíce vnímány ze strukturálních a procesních hledisek [8].

- **Strukturální** - Množina atributů charakterizující osobu.

- **Procesní** - Jedná se o soubor procesů týkajících se zveřejňování informací o osobě a použití těchto informací.

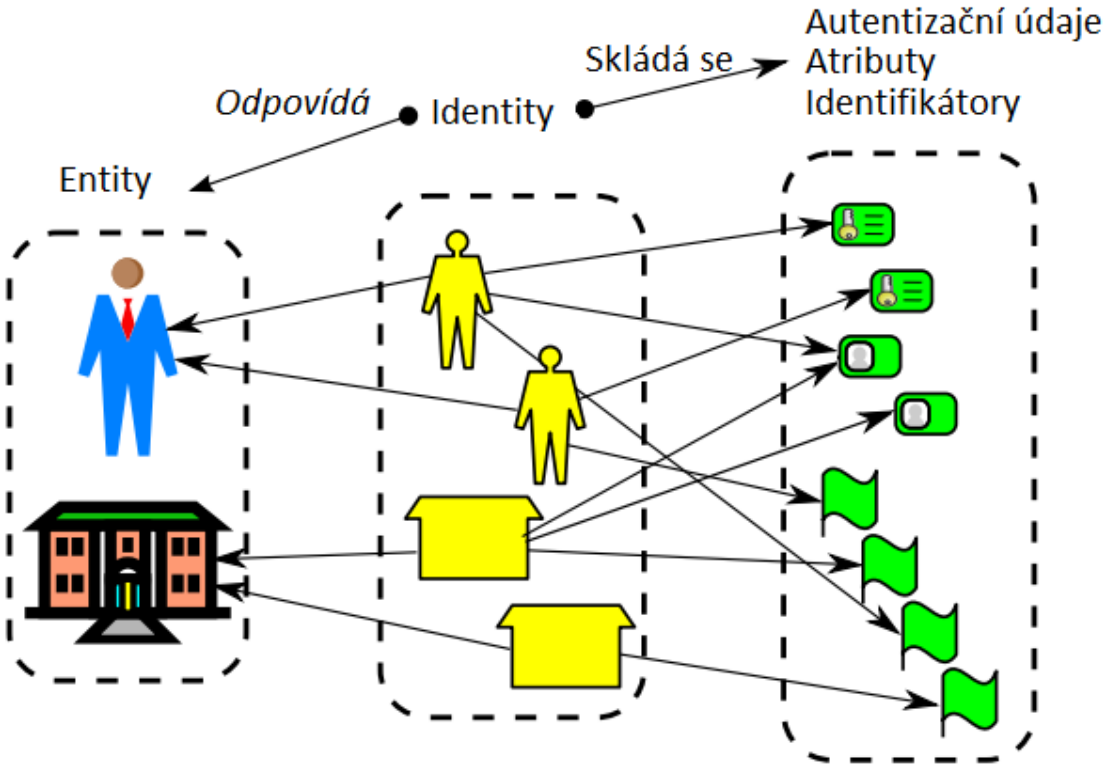
Poslední kategorizace je podle vlastníků a správců identit. Kontrola nad osobními údaji má zásadní význam v ochraně soukromí.

- **Medentity** - Identita je vázána na subjektu vztahem 1:1. Jde o pravou identitu. Identita nabývá platnost narozením člověka.

- **Ourtendity** - identita, jejíž existence závisí na vzájemných vztazích mezi subjektem a třetí stranou. Například uživatelský účet na herním portálu. Uživatel může vytvářet, upravovat a mazat uživatelský účet, ale herní portál má nad identitou určitou kontrolu založenou na všeobecných podmínkách.

- **Theirdentity** - Je identita, kterou třetí strana vytváří bez vědomého souhlasu subjektu. Tyto identity jsou generovány například pomocí cookies v internetovém prohlížeči a používají se k cílené reklamě.

Pokud jde o životnost, medentity trvá déle než ourdentity a theirdentity, protože poslední dvě jsou odvozeny od prvního. Subjekt může mít více než jednu identitu, z nichž každá představuje odlišnou charakteristiku. Z předchozích informací lze odvodit, že medentity je rovna entitě. Různé zdroje používají odlišné názvy [8].



Obr.č. 4: Teoretický model identity

Zdroj: Upraveno dle [9]

Obrázek ukazuje, že subjekt, jako jsou například osoby nebo organizace, může mít více identit a každý identity se může skládat z několika vlastností. Například totožnost identity „A“ jako firemního zaměstnance se skládá ze jména uživatelského účtu jako identifikátoru, znalostí hesla jako ověřovací údaj. Příjmení, seznam přátel, záznamů o činnosti jako atributy, které mohou a nemusí být jedinečné [9].

1.7 Identity management

Identity management (IdM) nebo také (IAM) je zkratka pro identity a access management (AM), což je samotná správa digitálních identit a řízení přístupu. IdM se ve většině případů chápe z hlediska použití v rámci organizace. V podnikovém IT slouží

správa identit pro řízení přístupu jednotlivce ke zdrojům a službám. I když jsou tyto systémy pevně začleněny se systémy kontroly přístupu, jejich hlavním cílem je propojit technické prostředky s organizační strukturou a pomoci správcům systémů i koncovým uživatelům s administrací přístupových údajů (uživatelské role a přístupová práva) ke kritickým podnikovým datům. Určení práva a přezkoumání těchto práv probíhá na rutinní bázi napříč různými funkčními jednotkami po celou dobu „identity lifecycle managementu“ (správou životního cyklu identit). Tento koncept zahrnuje množinu procesů a technologií potřebné pro distribuci zdrojů, či jejich správu a synchronizaci digitálních identit. IdM tedy automatizuje procesy vytváření hesel, účtů nebo změny účtů stávajících zaměstnanců. Automatizace procesů přináší redukci administrativních nákladů na obsluhu a přináší vyšší konzistenci dat mezi heterogenními systémy. Dále poskytuje nástroje, které umožňují monitorování činností uživatelů, změny rolí a dodržování nastavených politik. Jelikož disponuje vlastním uživatelským rozhraním, zkracuje lhůty pro vyřízení uživatelských požadavkům. Šetří tím čas uživatelům a administrátorům. Nasazení IdM do podnikové infrastruktury je poměrně složitá a komplexní záležitost. Je potřeba zaintegrovat technologie a aplikace do sebe. Propojit systémy, servery, zajistit jejich vzájemnou komunikaci a zavést školení pro všechny uživatele [10, 11].

Správa identit úzce souvisí s bezpečností. IdM systémy přispívají k ochraně digitálního majetku. Vlastnosti takových systémů umožňují centrální správu aspektů IT a ve společnosti mohou pomoci zjednodušit náročnost administrativních procesů. K dodržování bezpečnostní politiky přispívá centralizace systému [11].

1.7.1 Architektura

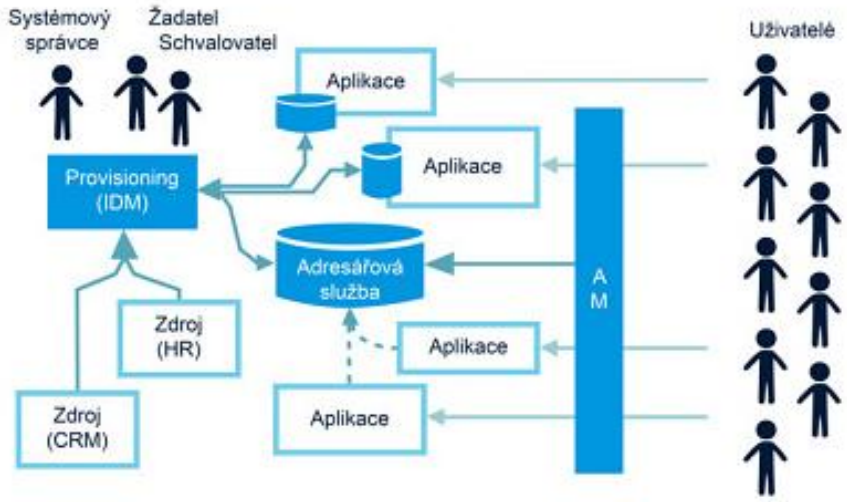
Správa identit a přístupů je založená na spolupráci více technologií. IdM tedy není jediný produkt, ale je to řešení složené z několika produktů. Každé řešení je sestaveno na míru pro potřeby organizace. I když se nasazení od sebe liší, existují tři technologie, které je možné najít téměř v každém řešení [12].

- Adresářová služba jako centrální databáze uživatelů.
- Systém řízení přístupů

- Provisioning zahrnuje proces tvorby identit, synchronizaci s databázemi a dodržování bezpečnostních politik.

Technologie se navzájem doplňují. Nelze je vynechat a ani zanedbat. Technologie jsou podrobně rozebrány v dalších kapitolách.

Typická architektura IdM je centrálně orientovaná, přičemž jednotlivé koncové systémy jsou s centrálním uzlem spojeny pomocí konektorů (agentů). Koncovými systémy jsou myšleny všechny aplikace či systémy, jež obsahují vlastní úložiště uživatelských účtů. Konektor lze chápat jako prostředek ke komunikaci mezi IdM a koncovými systémy. Obstarává operace jako řízení domovských adresářů nebo poštovních schránek. V dnešní době převažuje neinvazivní způsob komunikace. Jsou používány standardní protokoly a vrstvy. Například Secure Shell, LDAP. Způsob implementace konektorů je různá, záleží na konkrétním výrobci IdM. Výhoda tzv. neinvazivního způsobu je tom, že se nemusí ovládaný systém pro IdM přizpůsobovat. Konektory jsou od většiny výrobců v nejběžnějších koncových systémech předpřipravené. Snižují se tak náklady na vlastní vývoj řešení. Uživatelé se systémy komunikují buď prostřednictvím uživatelského rozhraní, nebo jiných aplikací. Koncové systémy si sami řídí autentizaci a autorizaci uživatelů. V následujícím obrázku je zobrazeno typické schéma architektury [10].



Obr.č. 5: Architektura IdM

Zdroj: [12]

IdM začne plnit svoji funkci příchodem nové identity (zákazník nebo zaměstnanec). IdM začne sledovat záznamy o identitě, ty se nejprve objeví v CRM nebo HR systému. Na základě zavedených politik přidělí novému uživateli přístupy. Nejdůležitější záznamy IdM vytvoří v adresářové službě. Když bude chtít uživatel získat přístup do koncového systému, Acess Management ověří jeho lokální identitu, jejíž záznam je v adresářové službě. Po ověření může uživatel pracovat s cílovým systémem [12].

1.7.2 Výzvy

Má-li být správa identit efektivní, musí se najít co nejlepší rovnováha mezi použitelností, bezpečností a soukromím. Každé navržené řešení vyžaduje různé přístupy s různými cíli. Některá řešení potřebují vysoká zabezpečení za cenu nižšího uživatelského komfortu. Někde je kladen důraz na efektivnost a použitelnost, ale za cenu nižší bezpečnosti. Je důležité, položit základy pro celistvé chápání problémových oblastí a synergické přístupy k inovativním řešením, jako jsou hlavní směry, metodiky, nástroje a technické normy. Klíčové otázky k řešení na správu identit jako základní disciplíny pro podnikání a společnost [8].

- Jak udělat identity dostupné pro správné osoby nebo služby, na správnou dobu a na správném místě?
- Jak vytvořit důvěru mezi stranami zapojených v transakcích identity?
- Jak zajistit, aby identita nebyla zneužita?
- Jsou tato ustanovení škálovatelná, použitelná a nákladově efektivní?

1.7.3 Výhody

Implementace IdM systému s použitím best practices může organizacím přinést konkurenční výhodu, efektivitu, zvýšení bezpečnosti a snížení nákladů. Výhody by se daly shrnout následujícím způsobem [11].

- Efektivní podnikání
    - Těsnější vztahy s dodavateli
    - Více flexibilní infrastruktura

    - Získání nových zákazníků
    - Jednodušší implementace organizačních změn
- Zvýšení bezpečnosti
    - Pevná bezpečnostní politika
    - Monitorování přístupu k aplikacím
- Snížení nákladů
    - Odstranění nadbytečné administrativy
    - Snížení zátěže help-desku
- Zvýšení produktivity
    - Zaměstnanci pracují rychleji
    - Administrátoři jsou volní pro další projekty
    - Single sign-on (SSO)
- Plnění předpisů regulačních orgánů

1.7.4 Nevýhody

I když v případě nasazení IdM převažují ve velkém výhody, každá změna vyžaduje nějaké úsilí a s tím plynou některé nevýhody. Mezi hlavní patří:

- Počáteční náklady na implementaci
- Nezbytná úprava firemních procesů
- Počáteční nároky na zaměstnance
- Riziko nedokončení projektu (Špatný výběr řešení, komplikace s dodavateli, apod.)

1.7.5 IdM framework

Doporučení ITU-T Y.2720 poskytuje rámec pro IdM v sítích nové generace (NGN). Rámec popisuje strukturovaný postup pro návrh, definování a implementaci IdM řešení a usnadňuje tím vzájemnou spolupráci systémů v heterogenním prostředí. Zabývá se řízením životního cyklu identity. Obsahuje rady, osvědčené postupy, zkušenosti. I když je určen pro NGN, je možné ho použít pro ostatní typy sítí [14].

1.7.6 Zainteresované strany

Existuje více stran, které mají zájem o digitální identity. Řešení pro IdM musí zohledňovat perspektivy každé takové strany. IdM tedy nebude uzavřený systém v jedné organizaci. Strany se kategorizují do čtyř skupin [8].

Subjekty

Jak už bylo několikrát zmíněno, subjekty jsou entity s identitami. Obsahují atributy, ověřovací údaje a atributy. Pro subjekty je klíčová ochrana osobních údajů [8].

Poskytovatelé identit

Poskytovatelé jsou strany, které poskytují identity subjektům. Plní čtyři základní úkoly:

- Vytvoří a přiřadí konkrétní atributy subjektu.
- Propojí přiřazené atributy s dalšími atributy subjektu.
- Generují tvrzení atributů.
- Poskytují ověřovací údaje k záznamům atributů.

Poskytovatel identit může propojit hodnoty atributů s jinými poskytovateli. Například člověk jako novorozenec získá identitu ve zdravotní pojišťovně. Má několik základních atributů, které se v čase mění, jako věk, místo bydliště. Později se jako absolvent vysoké školy zaregistruje na úřadu práce a získá nové atributy. Vytváří se tak nové závislosti atributů mezi zdravotní pojišťovnou a úřadem práce. Proto nestačí jen přidat nové atributy, ale propojit je s dřívějšími a aktualizovat je. Potom je možné generovat ověřovací údaje a tvrzení o atributech. To ale znamená, že subjekt musí

poskytovateli své údaje poskytnout a poskytovatel musí subjektu důvěřovat, že jsou pravé. Mezi poskytovateli musí být úroveň jistoty, protože si ověřovací údaje a atributy mezi sebou předávají [8].

Poskytovatelé služeb

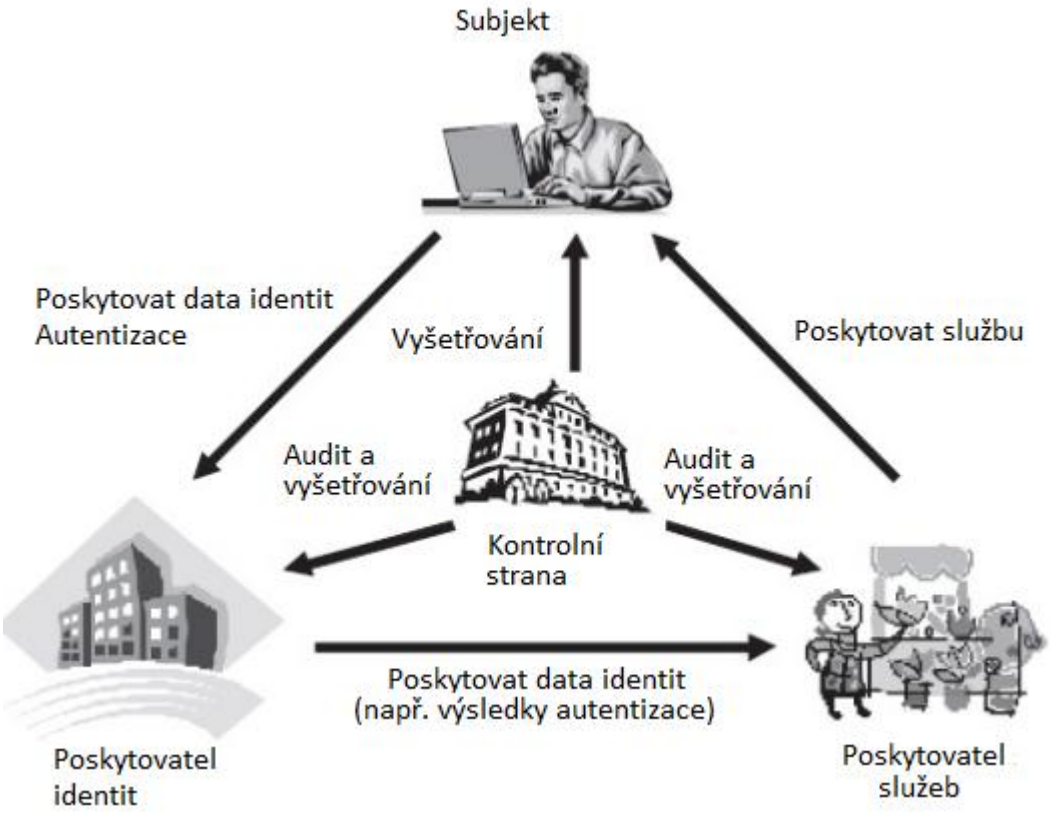
Jsou strany, které za účelem poskytování služeb uživatelům nebo přístupu ke zdrojům vyžadují ověřovací údaje. Důležitým úkolem těchto stran je určit, do jaké míry mohou ověřovacím údajům, atributům věřit. Zdroje či služby mají různé úrovně zabezpečení a přístupy vyžadují různé úrovně ověřovacích údajů. Tyto strany musí odpovídat předpisům a zákonům, jejichž cílem je zabránit krádežím identit [8].

Kontrolní strany

Kontrolní strany jsou obvykle donucovací a regulační orgány. V případě potřeby mohou požadovat přístup k informacím identity. Například transakční logy a další data pro forenzní šetření. Hlavním požadavkem od těchto stran je slyšitelnost a podpora v soudních procesech [8].

Vzájemné vztahy mezi stranami

Mezi stranami figurují určité vztahy. Zúčastněné strany IdM mohou mít více rolí. Například jeden účastník může mít obě role poskytovatele služeb a identit. Subjekt může být poskytovatel identit pro své vlastní identity. Mezi stranami mohou probíhat transakce identit i bez přímého souhlasu subjektů. Například cílené reklamy, založené na činnostech subjektů na webu. Konvenčně se každá strana stará sama o sebe. To přináší výhody a nevýhody. Podstatnou roli mezi stranami hrají použité standardy. V některých případech přenáší více odpovědnosti na jinou stranu a zbavuje odpovědnosti stranu druhou. Na obrázku jsou zobrazeny IdM účastníci a jejich vztahy.



Obr.č. 6: Účastníci IdM

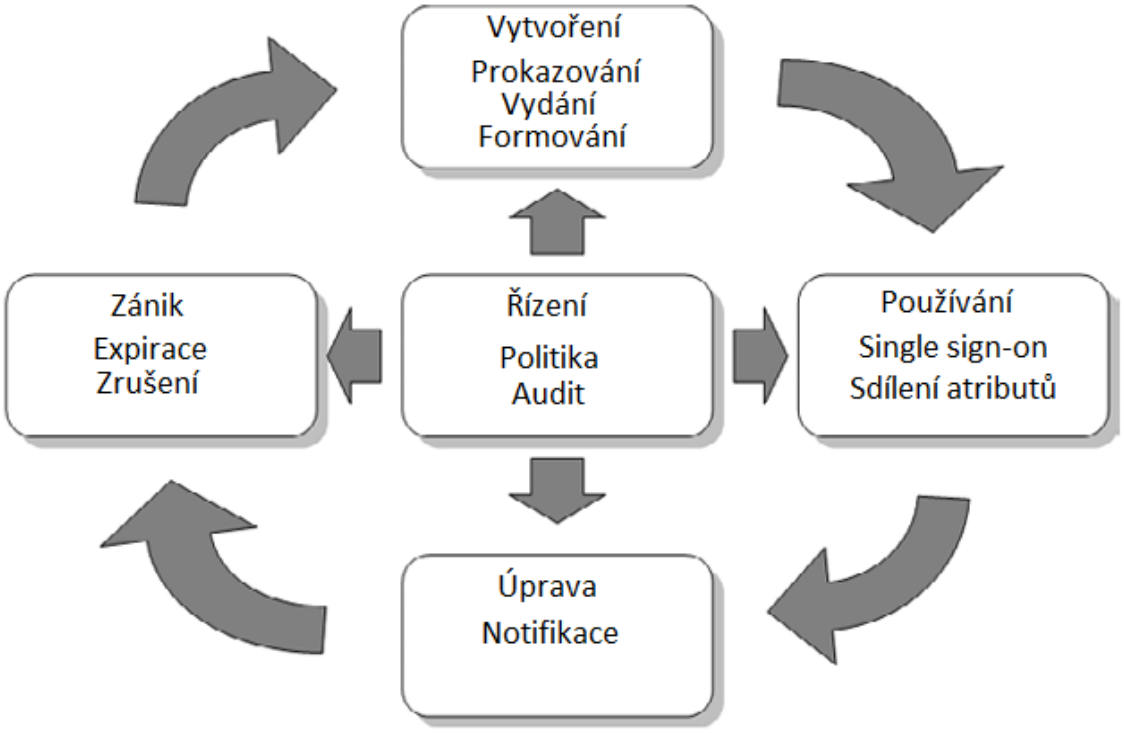
Zdroj: Upraveno dle [8]

1.7.7 Životní cyklus identity

Životní cyklus identity je základní proces IdM. Cyklus začíná nástupem zaměstnance do společnosti. Podle pozice v organizační struktuře mu jsou zřízeny uživatelské přístupy do aplikací. V průběhu času jsou uživatelská oprávnění přidávána nebo odebrána. Pokud zaměstnanec přeruší pracovní poměr, jsou jeho účty zneplatněny, tím je mu zabráněn přístup k aplikacím. Při obnovení pracovního poměru jsou účty znovu zpřístupněny. Pokud zaměstnanec odejde, jeho účty jsou vymazány a jeho identita zanikne. Životní cyklus identity má tyto fáze [10, 8].

- Vytvoření
- Používání
- Úprava
- Zánik

V životním cyklu identity hraje důležitou roli i řízení identity. Dále jsou jednotlivé fáze rozebrané podrobněji.



Obr.č. 7: Účastníci IdM

Zdroj: Upraveno dle [8]

Vytvoření

Vytvoření identity se skládá z tří dílčích kroků [8].

- **Prokazování atributů** - Je Prokazování atributů mezi autoritami. Například transakce, kdy si chce osoba koupit alkoholický nápoj, je požadován minimální věk 18 let. Některé transakce jako registrace na blogu být ověřeny nemusí.
- **Vydání ověřovacích údajů** - Po prokázání atributů je autoritou vydán ověřovací údaj. Například heslo nebo digitální certifikát.
- **Formování identity** - Nakonec se z identifikátorů, atributů a ověřovacích údajů vytvoří identita

Používání

Aby identity mohly využívat služeb, musí být jejich osobní údaje chráněny. K tomu se běžně používají tři funkce [8].

- **Důvěryhodná komunikace** - Pro důvěryhodné transakce mezi stranami je nezbytná důvěryhodnost identity. Stany by měli transakce rozpoznat důvěryhodným způsobem. K tomu zase potřeba důvěryhodná komunikace.
- **Single sign-on** - Je transakce identity, kdy subjekt jedinou autentizací získá přístup k více službám/aplikací.
- **Sdílení atributů** - Je transakce umožňující poskytovateli služeb a poskytovateli identit sdílet atributy subjektů. Zachovává integritu a eliminuje redundanci atributů.

Úprava

Data identity jsou v životním cyklu stále aktualizována. Například zaměstnanci vyprší platnost hesla. Nebo se zaměstnanec zapojí do nového projektu a jsou mu přidělena nová přístupová práva. Také údaje totožnosti by mely být stále aktualizovány. Například pokud člověk změní místo bydliště. Aktualizací dat se zajistí jejich integrita [8].

Zánik

Identity a ověřovací údaje by měly být zrušeny, pokud se stanou zastaralými nebo neplatnými. Zrušení je velmi důležité pro zajištění platnosti autentizace, autorizace a bezpečnosti celkově. Například pokud zaměstnanec podá výpověď, je třeba jeho identitu zrušit. Ověřovací údaje by měly být zrušeny, pokud vyprší jejich platnost, jsou ukradeny nebo narušeny. Tím se identita stane neplatnou [8].

Řízení

Celý životní cyklus by se měl řídit podle firemních politik a operace s identitami by měly být zaznamenávány. Řízení se dělí na dvě části [8].

- **Politiky** - v IdM se politiky týkají autentizace a autorizace, tedy řízením přístupu. Autentizační politiky definují požadovanou úroveň jistoty identity pro

danou transakci. Například identifikace pomocí hesla nebo pomocí hesla a tokenu. Autorizační politiky definují podmínky, za nichž je subjektům povolen přístup dané službě nebo datům. Každá zúčastněná strana může mít vlastní politiky.

- **Audit** - Životní cyklus identit by měl vytvářet záznamy a ty ukládat na centrální úložiště. Sběr dat a jejich analýza přispívá k vyšší bezpečnosti. Pokud systém detekuje akci, spustí se událost a ta vytvoří záznam. Cílem auditu je stanovit, zda jsou činnosti v souladu s bezpečnostní politikou.

1.7.8 Řízení přístupu

Technologie řízení přístupu je od ostatních IdM technologií odlišná tím, že uživatelům přímo vstupují do cesty. Každý uživatel by měl mít taková oprávnění a přístupy, které doopravdy potřebuje a měla být v pravidelných intervalech ověřována. Jednotlivá oprávnění a přístupy by měla být uživatelům přiřazena na základě analýzy rizik. U přístupu k aktivům se musí brát ohled na stupeň jejich bezpečnosti a uživatelského komfortu. V IdM se používají tyto technologie [15].

Single sign-on (SSO)

SSO je vlastnost informačního systému, která umožňuje uživateli přihlásit se jednou a získat přístup k více softwarovým systémů v rámci podniku (ESSO) nebo napříč více podniky známá jako multi doménová SSO. Přihlášení přes internetový prohlížeč jako Web SSO. Jednotné přihlášení má tu výhodu, že si uživatelé nemusí, pamatovat autentizací údaje pro různé systémy a aplikace. IT oddělení přináší výhodu ve výrazném snížení administrativních nákladů. SSO snižuje práce spojené s heslem, zjednodušuje vývoj aplikací, zvyšuje bezpečnost a dodržování politik. Z pohledu uživatele je SSO je vyhledávaným mechanismem, protože vyžaduje, aby si uživatelé pamatovali pouze jednu sadu ověřovacích údajů, většinou přihlašovací jméno a heslo uživatele. Z toho plyne, že zapamatovat si jedno silné heslo klade na uživatele menší zátěž, než si pamatovat několik různých hesel do různých aplikací. Nevýhoda spočívá v tom, pokud jsou uživateli odcizeny autentizací údaje. Útočník poté získá přístup k více aplikacím najednou. Existují různá řešení SSO [8, 16].

- **Zprostředkovaná architektura** - Hlavní úlohu plní centrální server, který ověřuje subjekty a poskytuje jim tickety. Pomocí těchto ticketů, mohou subjekty žádat o přístup k aplikacím. Příkladem je protokol Kerberos, SAML, OpenSSO, apod. Hlavní výhodou tohoto typu SSO je robustnost autentizace. Hlavní nevýhodou je obtížnější nasazení. I přes tento fakt se realizace stává snazší, neboť prodejci a vývojáři aplikací přijímají otevřené standardy, což přispívá k interoperabilitě aplikací.

- **Architektura s agenty** - Tento přístup je založený na autentizacích agentech. Agent se nachází na aplikačním serveru a chová se jako překladatel mezi protokoly autentizačního serveru a autentizačními údaji identity. Výhoda řešení spočívá v tom, že se není potřeba aplikace upravovat. Hlavní nevýhodou je možný problém synchronizace hesel mezi aplikacemi.

- **Reverzní proxy architektura** - V tomto přístupu je proxy server umístěný v demilitarizované zóně (DMZ). Filtruje, přesměrovává a řídí komunikaci mezi webovými servery a prohlížeči uživatele. Výhodou je anonymní přístup k sítí.

Jednotlivé prvky řešení architektur se mezi sebou dají kombinovat. Například řešení, které používá reverzní proxy architektury často vyžaduje, aby všechny aplikace, na něž se vztahuje proxy, byly schopny přijmout stejný mechanismus autentizace (například ticket Kerberosu).

Web SSO

Web single sign-on získává v dnešní době na významu. Na základě Web SSO modelu webové aplikace běží na různých aplikačních serverech a mohou sdílet stejné autentizací údaje. Uživatelé nejsou nepřetržitě vyzváni k zadání uživatelského jména a hesla při přechodu z aplikace do aplikace [16].

Role Based Access Control (RBAC)

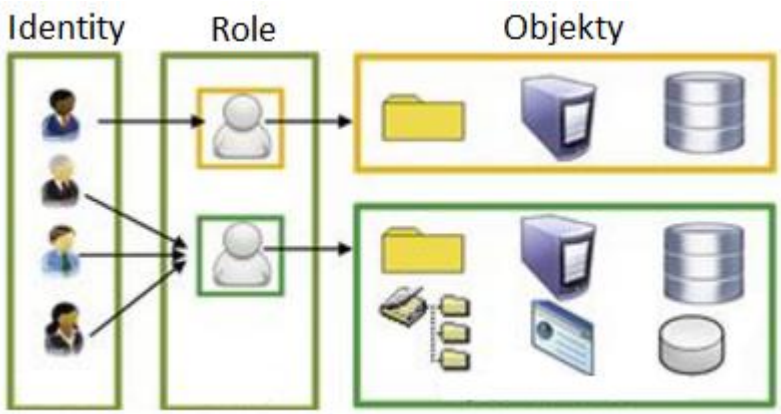
Uživatelé využívají podnikové systémy či aplikace k různým činnostem. Na základě autorizace mají přístupy k obsahu a činnostem. Oprávnění můžou být různá, záleží na typu koncového systémy. Jedná se profily, role nebo skupiny. Ve velkých organizacích, které disponují velkým množstvím systémů a aplikací, existuje velké

množství rolí. Nová oprávnění nabývají platnost, když se mění organizační zařazení nebo je zaveden nový systém. Je žádoucí oprávnění provázat s organizační strukturou a omezit jejich platnost podle jejich potřeby. V organizacích je nejrozšířenější princip řízení přístupu na základě rolí (RBAC). Role je sada přístupů a oprávnění k cílovým zdrojům. Typické role jsou zaměstnanec, zákazník, stážista, apod. [17].

Řízení přístupu na základě rolí je proces poskytování přístupu k systémům či aplikacím založenou na roli uživatele. Role každého uživatele jsou obvykle vázány na jeho pozici v organizaci. Jinými slovy, uživatel může mít více rolí na základě svého postavení nebo funkce v zaměstnání. Základní RBAC procesy jsou [16].

- Místo individuálního řízení uživatelů jsou definovány role.
- Uživatelé jsou přiřazeny k jedné nebo více rolím. Role odpovídají nastavení přístupových práv k jednotlivým zdrojům.
- Přístup uživatele ke zdrojům je založen na přístupových právech rolí, do které uživatel je přiřazen.
- Správci IdM budou spíše spravovat přístupová práva malého počtu rolí, než mnoho individuálních uživatelských oprávnění.

Následující obrázek znázorňuje vztahy mezi identitami, rolemi a objekty [16].



Obr.č. 8: RBAC model

Zdroj: Upraveno dle [18]

Přiřazení uživatelů k rolím a přístup do sítě, se nazývá mapování rolí. Jedná se o pracnou činnost, ale po dokončení, značně urychluje přiřazení přístupových práv uživatelům. Hlavním důvodem zavedení RBAC je redukce nákladů. Především snížení nákladů na správu řízení přístupu a správou adresářů. Dále šetří náklady v souvislosti lepšího řízení aktiv a zjednodušených postupů pro audit. RBAC také může výrazně urychlit odezvu organizace na strukturální změny. Kromě toho, RBAC umožňuje mapování zdrojů do podnikových procesů, což zlepšuje schopnost organizací optimalizovat obchodní procesy. Usnadňuje delegaci v rámci organizace. Pokud manažer dočasně deleguje svou roli na podřízeného, přístupová práva spojená s rolí se rychle a jednoduše přiřadí k zaměstnanci. Není nutné kontaktovat IT oddělení, aby přístupová práva měnila a v případě potřeby zrušila [16].

Podle NIST je RBAC model je rozdělen do čtyř úrovní pokročilosti. Vztahy modelů jsou definovány hierarchickou strukturou. Každá nadřízená úroveň obsahuje nové funkcionality [18].

- **$RBAC_0$** - Zaměřuje se na oprávnění uživatelům již v rámci role. Je základní model a nepodporuje hierarchickou strukturu.

- **$RBAC_1$** - Staví na RBAC0 s podporou hierarchie. Zavádí koncept úrovní odpovědnosti dané pracovní pozici. Nadřazená role se nazývá „senior role“ a podřazená role „junior role“. Mezi rolemi funguje tranzitivní dědičnost oprávnění. Například ředitel zdědí všechna oprávnění po podřízených. Z toho plyne nevýhoda, že nepodporuje omezení oprávnění.

- **$RBAC_2$** - Neobsahuje podporu pro hierarchii jako $RBAC_1$, ale zavádí pojem omezení. Omezení působí jako donucovací mechanismus pro omezení přístupu či členství v dané roli. Toho lze dosáhnout zavedením různých pravidel. Například model může být nastaven tak, že senior role nemůže být přiřazena k uživateli, pokud junior role byla přidělena jako první.

- **$RBAC_3$** - Obsahuje všechny aspekty $RBAC_1$ a $RBAC_2$. Umožňuje vytvářet omezení v souvislosti s hierarchií. RBAC3 je nejkomplexnější a detailní model řízení přístupu na základě rolí.

Hlavní motivací pro vybudování hierarchie rolí je fakt, že se oprávnění rolí často překrývají. Zavedení hierarchie má dvě výhody. Za prvé je vytvořena lepší představa jaká oprávnění jsou přiřazeny které roli a za druhé se může snížit počet rolí [16].

RBAC také zabraňuje tzv. „toxickým“ kombinacím přístupu. To zajišťuje mechanismus Separation of Duties (SoD). Jedná se o bezpečnostní politiku, která stanovuje, že žádný jedinec nemůže provést všechny transakce v rámci souboru. Například jedna a ta samá osoba by neměla zadat příkaz pro platbu a také ji schválit. Transakci tak dokončí určitá množina osob. SoD se dělí na statické a dynamické. Například pro dokončení platby jsou potřeba dvě transakce, jedna pro zadání a druhá po schválení platby. Každá transakce obsahuje samostatnou roli. U statických SoD nemůže být uživatel členem obou rolí. U dynamických uživatel může být členem obou rolí, ale je zakázáno schvalovat transakce, které uživatel sám vytvořil. Jsou tedy více flexibilní, ale díky komplexnosti složitější na implementaci [19].

Existují další alternativy řízení přístupu [18].

- **Mandatory Access Control (MAC)** – Přístupová práva jsou definována správcem objektu a nemohou být změněna koncovými uživateli. Používá se například ve vojenských objektech, kde jsou kladeny vysoké požadavky na bezpečnost. Jsou náročná na administraci.

- **Discretionary Access Control (DAC)** – Umožňuje uživatelům přidělovat oprávnění dalším osobám.

- **Attribute Access Control – (ABAC)** – Řídí přístupy na základě atributů. Například identitě je povolen přístup, pokud dosáhla 18 let.

1.7.9 Adresářové systémy

Adresářový systém je důležitou komponentou IdM. U menších IdM řešení se používá Active Directory. U větších řešení není Active Directory jediná databáze identit. Adresářové systémy poskytují jednotný a unifikovaný pohled na kritická data identit a slouží jako jejich uložiště. Součásti systému v rámci celé organizace je sběr těchto informací. Adresářové systémy mají hierarchickou strukturu, jsou standardizovány a navrhovány na masivní škálovatelnost. Jejich datový model je velice

jednoduchý a jsou omezena na data, která se v nich ukládají. Systémy jsou velice rychlé, ale nevýhodou je omezená administrace. Správa až milionu zákaznických identit by byla příliš drahá. Služba poskytuje jednoduchý systém vnořených skupin. To má za následek, že řízení přístupu RBAC není podporováno takřka vůbec. Systémy jsou tvořeny alespoň dvěma servery, můžou proto replikovat svůj obsah a zajistit vysokou dostupnost. Jsou proto ideální na ukládání údajů o identitách. Údaje se zřídka mění a často čtou. Díky vysoké dostupnosti je zajištěno, že se uživatel do systému vždy přihlásí. Je to rychlá, dostupná a škálovatelná databáze identit [16, 20].

Součástí adresářových systémů je Meta-adresář, který poskytuje v reálném čase transformace dat a řízení změn v různorodých adresářů, databází a aplikací. Většinou se skládá s agentů, kteří dohlíží na změny v jednotlivých systémech. Poskytuje základ pro IdM rámec, který umožňuje společnostem reagovat rychle na měnící se podmínky [16].

Standardem adresářových systému se stal LDAP protokol. Díky standardizaci se aplikace s těmito systémy snadno integrují. LDAP je možné použít i jako autentizací protokol. To je vhodné pouze pro malá řešení, jelikož adresářové systémy neudržují informace o relaci a nelze proto použít SSO. To je důvod, proč složitější IdM řešení potřebují technologii řízení přístupu. Adresářové systémy primárně neslouží jako zdroj informací. Od toho tu jsou databáze. Zdroje dat s adresářovými systémy je potřeba synchronizovat. K tomu slouží technologie provisioning [20].

1.8.0 Provisioning

Provisioning je základním prvkem pro správné fungování IdM. Je to proces vytváření uživatelských účtů, stanovení oprávnění, rolí a dalších úkolů na základě požadavku administrátora a automatických změn v systémech. Snižuje tak náklady a ulehčuje administrátorům práci ve vytváření a udržování účtů. V důsledku velkého počtu ručních zásahů může dojít k mnoha chybám. Účty se vytvářejí a ruší pozdě nebo vůbec. Zaměstnanec, který podá výpověď a nemá zrušený účet, může společnosti způsobit velké škody. Mnoho administrátorů používá poloautomatická řešení založená na skriptech. Je to sice lepší způsob než provádět činnosti manuálně, ale nikdy se tím nepokryjí všechny systémy a události. Pro plně automatické řešení musí být správně nakonfigurovány identifikátory, role/skupiny a autentizační údaje [18, 21].

- Identifikátory - Bez standardního uživatelské ID není možné přiřadit přístup v koncovém systému.
- Role/skupiny - Musí existovat jasné mapování skupin, rolí.
- Autentizační údaje - Ověřovací údaje musí být uloženy v centrálním úložišti.

Vytvoří-li se v provisioning systému nová identita, automatická synchronizace přidělí v dalších systémech identitě přístupová práva dle stanovených politik. Automatické synchronizace na ostatních systémech kontrolují, jestli nedošlo k bezpečnostním incidentům a starají se rekonciliaci identit. To znamená, že identifikují přístupy, které byly vytvořeny manuálně, a kterým neodpovídá žádná role. Na nesrovnalost je upozorněn administrátor [21].

Opakem provisioningu je de-provisioning. Při tomto procesu se ukončí přiřazení identit k systémům a službám.

Workflow

Nedílnou součástí provisioningu je workflow. Je to systém, který spravuje sled úkolů procesů konkrétním osobám nebo systémům. V rámci IdM systémů workflow řídí žádosti. Jakmile je podána žádost, systém workflow přesměruje požadavek na příslušné jednotlivce ke schválení a poté předá schválení provisioningu. Workflow systémy určené pro IdM jsou vybaveny uživatelským rozhraním, které pomáhá uživatelům identifikovat typ přístupu, které potřebují a podání žádostí k příslušným osobám. Systém je často předem nakonfigurován, aby požadavky k vhodným osobám přímo směroval. Například manažer lidských zdrojů schválí přidání nového zaměstnance do adresáře. Obchodní manažer bude schvalovat přístupy ke sdíleným souborům. Pokud zaměstnanec bude chtít citlivá obchodní data, podá žádost, která se přesměruje k obchodnímu manažerovi. Ten může, ale nemusí žádost schválit. Lze říci, že workflow rozděluje proces na menší části postupných kroků [18].

1.8 Trezory hesel

Pokud je v organizaci hodně systémů a není zaveden systém jednotného přihlášení, nastává problém se správou hesel. Uživatelé si tak musí pamatovat několik hesel. Podle firemních politik většinou hesla nesmí být stejná, musí mít minimální počet znaků,

apod. Pro uživatele je tak jednodušší si hesla zapsat buď v papírové podobě nebo v elektronické například do programu MS Word nebo Excel. Trezor hesel je tedy aplikace, která uživatelům pomáhá bezpečně ukládat hesla. Většinou je vyžadováno jedno přístupové heslo, které si musí uživatel pamatovat a po jeho zadání získá přístup k ostatním heslům. Trezory jsou buď uložené na pracovní stanici (offline) nebo na vzdáleném serveru (online). Výhoda prvního spočívá v tom, že jsou hesla uložená na pevném disku počítače a uživatel má hesla přímo u sebe. Pokud se však chce uživatel ke svým heslům dostat z jiného počítače, trezor musí mít stále u sebe například v podobě USB flashdiku. U online trezorů jsou hesla přístupná odkudkoli. Jsou však uložená na vzdáleném serveru a uživatel nemá hesla u sebe. Je tedy potřeba mít přístup k internetu. Online trezory mají podobu doplňků internetových prohlížečů nebo webových aplikací. Existují i řešení, která umí obojí. Jsou nainstalovány na pracovní stanici a ukládání do cloudu se v aplikaci vypne nebo zapne. Další možnost je synchronizovat hesla přímo mezi zařízeními a hesla se do cloudu neukládají. Řešení může být také postaveno na centralizované databázi v podniku, nejedná se však o robustní řešení pro tisíce uživatelů. Některé trezory jsou k dostání s otevřeným zdrojovým kódem tzv. open source. Používají silné šifrovací algoritmy AES, Twofish, Serpent, RC4, apod. Standardní délka klíče je 256bit. Požadavky na trezory se mohou lišit. Například běžný uživatel bude chtít aplikaci, ke které se připojí odkudkoli. Hesla se mu budou automaticky vyplňovat do webových formulářů a aplikací. Ve firmě může být situace trochu jiná. Ve směrnicích společnosti může být například uvedeno, že hesla se nesmí ukládat na vzdálené servery. Zde připadá v úvahu offline správce hesel. Součástí trezorů bývají další funkce [24]:

- Více faktorová autentizace – Trezor je chráněn hlavním hesel. Dále například jednorázovým heslem a pomocí USB tokenu.
- Automatické vyplňování formulářů – Autentizační údaje, které jsou uloženy v trezoru, se automaticky vyplňují do webových stránek.
- Automatická změna hesla – Hesla se automaticky mění podle časových intervalů.

- Import/Export – Jaké formáty jsou povolené pro import/export hesel. Například textové soubory, soubory csv, HTML.
- Sdílení hesel – Sdílené hesel s ostatními uživateli buď uvnitř, nebo vně trezoru hesel.
- Bezpečnostní audit – Správce hesel odhalí slabá hesla.
- Podpora aplikací – V aplikacích jsou hesla automaticky vyplňována podle hesel z trezoru.
- Bezpečnostní politiky – Různá omezení. Například základ importu/exportu souborů a zákaz instalace doplňků.
- Generátor hesel – Trezor má vlastní generátor, který vytváří hesla podle nastavených pravidel.
- Virtuální klávesnice – Ochrana proti odposlouchávání kláves Keylogger.
- Psaní bezpečnostních poznámek – Do správce hesel je umožněno ukládat vlastní poznámky jako PINY, čísla platebních karet, apod.
- Kompatibilita s operačními systémy – Podpora operačních systémů Windows, Linux, Mac OS X, BSD, Android, Windows Phone, apod.

2 Analýza současného stavu

V rámci analýzy se budu řídit doporučeními normy ISO/IEC 27001. Zaměřím se na kapitoly:

- A.9.1 – Požadavky organizace na řízení přístupu.
- A.9.2 – Řízení přístupů uživatelů.
- A.9.3 – Odpovědnosti uživatelů.
- A.9.4 – Řízení přístupu k systémům a aplikacím.

Prošetří se tak aktuální stav IdM ve společnosti. Dále provedu analýzu procesů, které souvisí s životním cyklem identit. Součástí bude také zmapování trhu trezorů hesel.

2.1 Charakteristika společnosti

Kvůli utajení informací si společnost nepřála být jmenována, v práci ji budu nazývat XYZ.

Společnost XYZ je poskytovatelem řešení a služeb informačních technologií s dlouhou tradicí inovací. Převažující činností XYZ je prodej širokého spektra IT technologií od serverů a systémů pro ukládání dat až po software a IT služby včetně služeb konzultačních. Tržby společnosti dosahují v průměru několik stovek mil. Kč a počet zaměstnanců je několik tisíc.

K hlavním cílům společnosti XYZ patří poskytování komplexních služeb systémového integrátora a prosazování výhod elektronického obchodu do každodenního života firem. Integrální součástí strategie XYZ jsou také programy firemní společenské odpovědnosti, jimiž XYZ přispívá k řešení ekologických a sociálních problémů společnosti.

Pobočka se sídlem v Brně, na kterou se vztahuje tato práce, byla založena v roce 2001. Její hlavní aktivity jsou zaměřeny na poskytování strategických outsourcingových služeb - vzdálená správy IT, jako je například instalace serverů, správa sítí, podpora aplikací a nepřetržitý dohled nad jejich během nebo koncová podpora pro zákazníky, kterých je více než 600.

Společnost má certifikaci managementu kvality ISO 9001, řízení IT služeb ISO/IEC 20000-1 a řízení informační bezpečnosti ISO/IEC 27001. Výhody pro klienty, na kterých si společnost zakládá jsou:

- Inovativní a integrované přístupy k dodavatelským službám
- Rozsah znalostní a působností společnosti
- Plný rozsah servisních služeb s možností využití globálních výzkumných center a laboratoří
- Schopnost pokrýt vzrůstající se požadavky a flexibilně reagovat na jejich změnu
- Vysoká výkonnost na bázi SLA smluv
- Zkušenosti s vedením lidí
- Globálně dodavatelský model snižuje rizika

2.1.1 Organizační struktura

Organizační strukturu tvoří týmy o průměru 30 lidí. Za vedení týmu je zodpovědný team leader, který vykonává administrativní práce a zajišťuje týmu podporu. Team leader se zodpovídá svému nadřízenému, tzv. 1st line manažerovi. Pro společnost je typické decentralizované řízení a je řízena generálním ředitelem. Přístup se přiděluje na základě role, kterou tzv. approval manager potvrdí na základě business needs uživatele.

Obr.č. 9: Organizační struktura

Zdroj: Upraveno dle [23]

2.2 Bezpečnostní politika

Společnost prošla certifikací ISMS v roce 2013. Společnost používá vlastní firemní politiky, které jsou v souladu s normou ISO/IEC 27001:2013 a zaměstnanci jsou povinni je dodržovat. V roce 2014 prošla kontrolním auditem a v roce 2015 recertifikací podle nové verze normy ISO/IEC 27001:2013. Auditor doporučil zlepšení v oblastech:

- Řízení přístupu. Konkrétně odstranit duplicitní rolí v systému.
- Mobilní zařízení a práce na dálku. Odstavec ve směrnici o používání mobilních zařízení se nevztahoval na externí mobilní telefony, pouze interní.
- Řízení rizik

Silné stránky:

- Matice SoD.
- Dobře navržený systém pro měření efektivnosti.
- Průvodce pro nasazení kompetence managementu.

Aby nedocházelo k obcházení procesů, kontroluje se jejich funkčnost a plnění požadavků s ISO 27001.

2.2.1 Řízení přístupu

Požadavky organizace na řízení přístupu

Společnost má vypracované dokumenty politiky řízení přístupu. Tyto politiky jsou zaměstnanci povinni dodržovat. Přístupová práva jsou zaměstnancům přidělena na základě rolí. Práva přiděluje kompetentní osoba na základě business needs pracovníka na dobu, po kterou práva potřebuje. Přidělené role jsou dohledatelné a monitorované.

Zaměstnanci mají přístup do internetu a intranetu, mají možnost využívat sdílené tiskárny. Z pracovních stanic, které jsou připojené do firemní sítě, je administrátorům zakázáno přistupovat na webové stránky, které nesouvisí s pracovní činností. Je možné stahovat pouze software, který je ověřen na stránkách společnosti. Je zakázáno používat jakékoli nástroje pro monitorování sítě, bez souhlasu správce sítě. Návštěvníci mají zakázáno přistupovat do firemní sítě z pracovních stanic zaměstnanců. Návštěvníci

mohou do sítě přistupovat prostřednictvím bezdrátové sítě pro ně určené. Do firemní sítě se mohou přihlásit pouze registrovaná zařízení.

Řízení přístupu uživatelů

Registrace zaměstnance probíhá pověřenou osobou v HR systému. Vytváření identity probíhá z přednastaveného provisioningu. V případě, že zaměstnanec ukončí pracovní poměr, je odstraněn z tzv. modrých stránek společnosti a okamžitě mu zaniká přístup do intranetu a emailové schránky. Přístupová práva jsou pravidelně přezkoumány pověřeným pracovníkem, intervaly a procesy s tím spojené budou rozebrány v další kapitole. Za odebrání přístupových práv je zodpovědný nadřízený zaměstnance. Manažer zaměstnance je vždy informován, aby ID uživatele na serverech smazal. Ze systému mohou být odebrána pouze taková přístupová práva, která zaměstnanci nebrání k vykonávání business needs. Taková situace může nastat, pokud zaměstnanec přechází mezi odděleními a mění pracovní pozici. Při přechodu zaměstnance do jiného oddělení, závisí odebrání práv na současném manažerovi, který je na celou situaci upozorněn emailem.

Použití tajných autentizačních informací

Hesla jsou držena v tajnosti a je zakázáno sdílení s ostatními uživateli. Každý uživatel je zodpovědný za všechny aktivity, které vykonává v rámci svojí identity. Ve směrnicích společnosti není uvedeno, jakým způsobem má být heslo uloženo, pokud si to situace vyžaduje.

Řízení přístupů k systémům a aplikacím

Společnost má zavedený systém pro správu hesel. Heslo musí splňovat následující požadavky:

- Nesmí být předvídatelné.
- Délka minimálně 8 znaků.
- Musí obsahovat mix znaků abecedy a speciální znaky (např. h1k8lko45io) nebo alespoň 2 speciální znaky (např. 13%7@88_).

- Nesmí obsahovat ID uživatele jako součást hesla.
- Maximální trvanlivost hesla je 90 dní.
- Nelze použít stejné heslo do interních a externích systémů

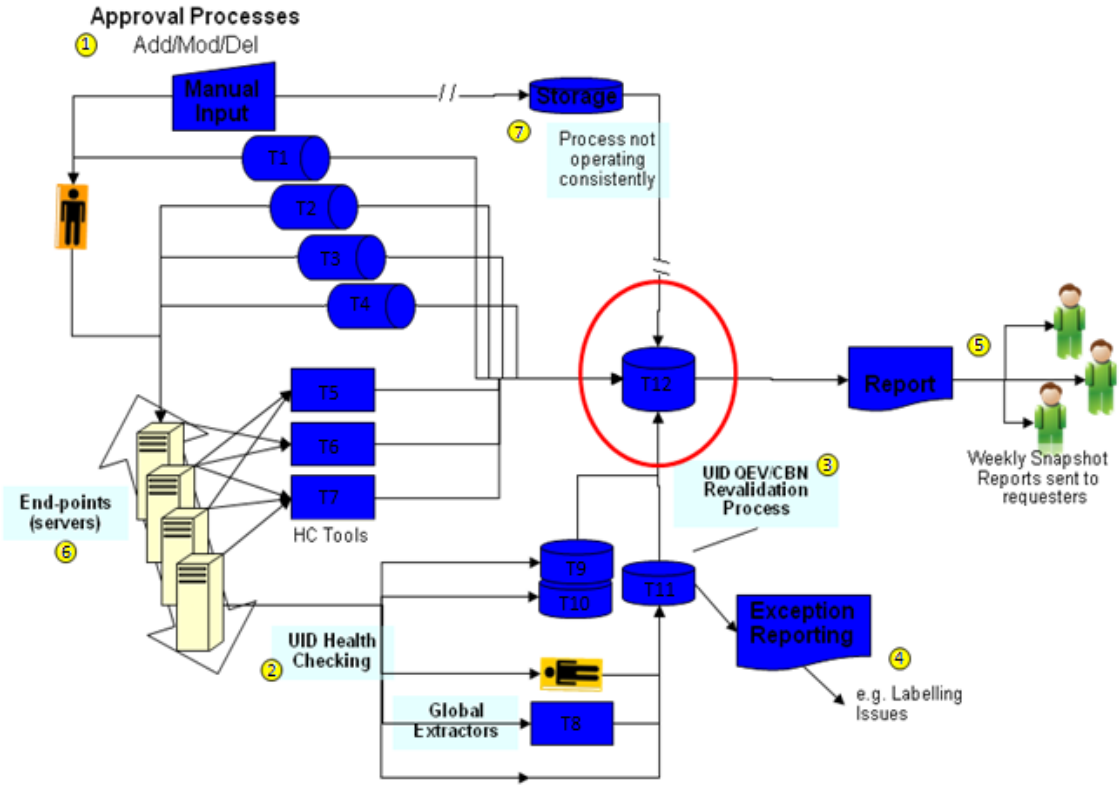
V případě, že si zákazník nepřeje nebo nemůže splnit politiku hesel, sepisuje důvod, popisuje se riziko a odpovědnost. Některé starší systémy neumí speciální znaky v hesle nebo ignorují velká písmena. Pokud uživatel použije stejné heslo, které již v minulosti použil, musí být splněny další podmínky. Platnost hesla je minimálně jeden den a stejné heslo může být použito znovu, až se protočí dalších osm hesel. Tato funkce závisí na možnosti platformy, zda ji umí. Ve společnosti jsou některé staré systémy, kde tato možnost nastavit nejde. Z pohledu uživatele probíhá změna hesla dvojím způsobem. Intranetové heslo změní uživatel zadáním emailu na webových stránkách společnosti. V šifrované podobě mu přijde odkaz na stránku, kde si heslo může změnit. Pokud chce heslo změnit na serveru/doméně/systému/firewallu, tak změna probíhá přes nástroje IdM. Do něj se přihlásí, vybere si server, kde chce heslo změnit. Pokud si heslo nechá vygenerovat, přijde mu emailem, pokud si ho zvolí sám, přijde mu potvrzení o změně hesla. Do nástroje IdM se uživatel dostane přes intranetové heslo.

2.3 Identity management ve společnosti

Společnost vlastní více nástrojů pro správu identit. To je způsobeno tím, že poskytuje své služby mimo Českou republiku a její zákazníci mají různé preference. Dalším důvodem jsou akvizice společnosti. I když jsou řešení do jisté míry heterogenní, jsou mezi sebou provázané a komunikují spolu, i když ne na plnohodnotné úrovni. Heterogenita systémů si však vybrala svoji daň. Tou je absence technologie jednotného přihlášení. To sebou nese problém ukládání hesel. Ve společnosti zaměstnanci přistupují do několika stovek systémů. Je nereálné si všechna hesla pamatovat, protože z hlediska politik jsou na ně kladeny požadavky v počtu znaků, kombinace velkých, malých písmen a speciálních znaků. Je zde riziko, že zaměstnanci budou hesla ukládat v nešifrované podobě například v MS Excel, poznámkovém bloku, apod.

Do jednotlivých nástrojů jsou implementovány politiky, které hlídají, zda je zaměstnanec stále zaměstnancem. U novějších nástrojů je kontrola QEV (Quarter Employment Verification) prováděna denně, u manuálních kvartálně. Tím se ze

systémů odstraňují spící účty identit. Jedenkrát ročně probíhá hloubková kontrola CBN (Continuing Business Needs). Ta zajistí, že všechny uživatelská ID mají správně přidělená oprávnění. Pokud je nějaký systém vyřazen z provozu, spustí se proces, jehož tým má za úkol server odstranit. Současný IdM systém je částečně sledován z pohledu bezpečnostních slabin. Společnost plánuje postupně nahrazovat staré systémy novými. Na novou verzi systémy se přejde, až bude kompletní migrace starých systémů. V IdM systému jsou logovány aktivity uživatelů a administrátorů. Lze, tedy zpětně dopátrat, kdo co v systému provedl. V následujícím obrázku je zobrazeno propojení IdM nástrojů.



Obr.č. 10: Architektura nástrojů

Zdroj: Upraveno dle [22]

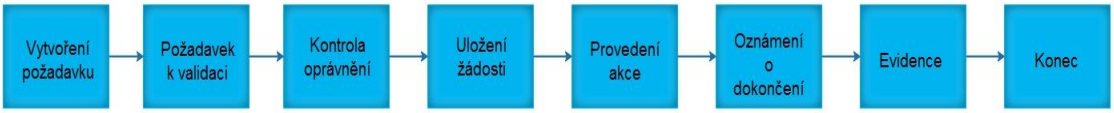
Diagram architektury poskytuje přehled standardizovaných nástrojů pro správu identit. Proces začíná žádostí uživatele (1), který vyžaduje přístup k jednomu, či více serverů (6). Tento požadavek vzniká manuálně, buď pomocí různých nástrojů nebo přímo na serveru. Jakmile je provedena tato akce, uživatelské ID se může stát předmětem procesu revalidace CBN a QEV (2) a (3). V nástroji T11 probíhají

revalidace identit. T11 také sbírá data od nástrojů kontrolující „zdraví“ identit (2), posílá data do T12. T12 je centrální uložiště dat pro následné reporty kontrolním týmům.

Servis IdM je rozdělen mezi tzv. primární, sekundární kontrolu a Shared ID management. Share ID management je více specifický, odpovídají mu jiné procesy a není předmětem této práce. Procesy jako vytváření, úprava, odstranění identit a reset hesla, probíhají pomocí přednastavených workflow.

2.3.2 Proces primární kontroly

Týmy primární kontroly řídí životní cyklus identit. Tyto kontroly se vztahují k identifikaci, autentizaci a autorizaci, včetně rutin provisioningu jako na příklad přidání, úprava, přenos nebo odstranění ID, skupin, nebo oprávnění v různých systémech a aplikacích. Patří sem i správa hesel. Proces je tvořen následujícími kroky:



Obr.č. 11: Proces primární kontroly

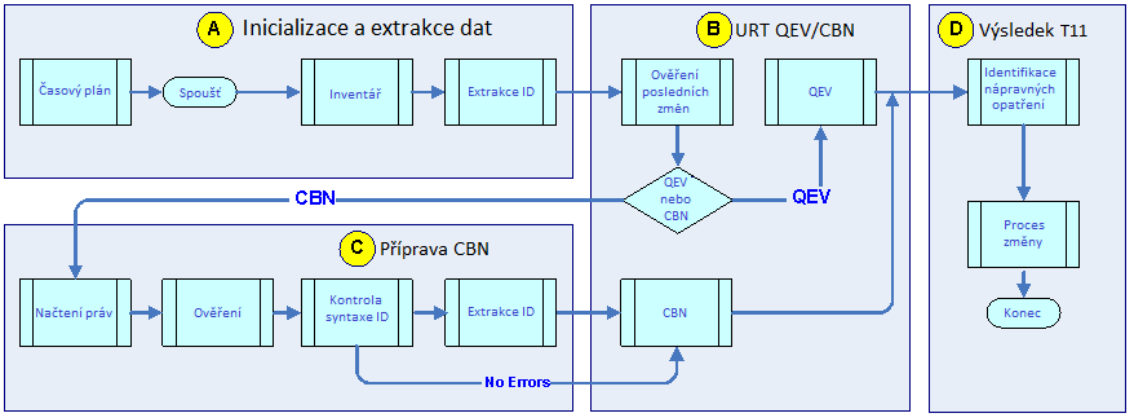
Zdroj: Upraveno dle [22]

Uživatel vyplní formulář k žádosti, ke které dostane přístup od svého liniového manažera. Žádost se odesílá IdM týmu, který ji ověří. Pokud je zamítnuta, je o tom uživatel informován. Potom se v HR systému společnosti ověřuje, má-li uživatel na žádost patřičnou autorizaci. Po schválení je žádost zaevidována a to na nejméně 2 roky. Nyní tým vykoná patřičné kroky, o které uživatel zažádal. Jak již bylo zmíněno, může to být cokoli, co souvisí s cyklem řízení identit. Například změna oprávnění, reset hesla apod. Uživatel obdrží oznámení o vykonání akce. Všechny předešlé kroky se zaevidují a proces končí. Záznam slouží pro audit.

2.3.3 Proces sekundární kontroly

Sekundární kontrola detekuje selhání v primárních kontrolách. Někdy se stane, že manažer zapomene nahlásit odchod zaměstnance na jiné oddělení, změnu rolí nebo jsou špatně nastavena oprávnění. Mezi hlavní úkoly patří kontrola pracovního poměru

(QVE) a správné nastavení oprávnění pro vykonávání business needs (CBN). Proces revalidace se skládá z následujících kroků:



Obr.č. 12: Proces primární kontroly

Zdroj: Upraveno dle [22]

Celý proces se řídí podle časového plánu, který je nastaven podle politik. Ve fázi „A“ probíhá příprava dat. Zjišťuje se, které ID se budou revalidovat. Vše je monitorováno a data jsou načtena do nástroje T11, kde celý proces probíhá. Ve Fázi „B“ se nejprve ověří poslední změny v ID. Podle záznamu o ID se zjistí, o jaký typ kontroly se bude jednat. Bude-li se jednat o kontrolu QEV, na modrých stánkách společnosti se ověří ID zaměstnance. Kontrola CBN probíhá ve fázi „C“. Aby celá fáze proběhla úspěšně, musí být splněny podmínky: Identifikace oprávnění uživatele, vlastník oprávnění stále vykonává svoji roli a atributy ID musí být správně vyplněny. Aby mohl být celý proces kompletní, v poslední fázi se vše zaeviduje a proběhne reporting příslušným osobám. Jedná-li se o zákazníka, reporting probíhá na základě SLA smluv.

2.4 Požadavky zadavatele

Společnost XYZ chce provézt analýzu identity managementu, zda plní požadavky normy informační bezpečnosti. Požaduje také analýzu procesů, které se řízením identit souvisí. Společnost chce zavést systém jednotného přihlášení, až budou IdM nástroje konsolidovány. SSO tedy nebude součástí návrhu řešení.

2.5 Dostupné trezory hesel

Na trhu existuje celá řada trezorů hesel. V této kapitole budou popsány nejčastěji používané.

LastPass

LastPass je jeden z nejpoužívanějších trezorů hesel a patří mezi online správce. Existuje verze Free, Premium (12USD ročně) a Enterprise (24 USD ročně). Verze free je doplněk internetového prohlížeče a ostatní verze mají podobu webové aplikace. Základní verze obsahuje základní generátor hesel, psaní bezpečnostních poznámek, automatické vyplňování formulářů, více faktorovou autentizaci, automatické odhlášení, virtuální klávesnice a import/export souborů. Členové komunity mohou hesla mezi sebou sdílet. Databáze je šifrovaná algoritmem AES. Verze prémium je navíc obohacená o synchronizaci mezi zařízeními a je kompatibilní s mobilními telefony. Verze Enterprise podporuje systém jednotného přihlášení. Uživatelské rozhraní působí moderním dojmem [25].

Passpack

Passpack je další online správce hesel ve formě webové aplikace. Je dostupný v pěti verzích. První verze free je zdarma. Další verze se liší počtem uložených hesel, velikostí uložených poznámek a počtem sdílení mezi uživateli. Ve verzi free si uživatel uloží 100 hesel. Cena verzí se pohybuje od 1.5 USD až 40 USD za měsíc. Uživatelé mohou posílat zabezpečené zprávy ostatním uživatelům. Passpack obsahuje generátor hesel, dvou faktorovou autentizaci, funkci automatického odhlášení, virtuální klávesnici a šifrování pomocí algoritmu AES. Import/export souborů je bohužel bez podpory formátu excel [26].

Roboform

Roboform má více jak 3 milion uživatelů a je přeložen do 30 světových jazyků. Řešení pro desktopy je zdarma nebo ve verzi everywhere. Další řešení jsou cloudová nebo podniková. Ve verzi free lze uložit maximálně 10 hesel a pro synchronizaci hesel mezi více zařízeními je potřeba verze Roboform Everywhere, jejíž cena je 20 dolarů ročně. Podporuje vytváření více identit pro snadnější vyplňování formulářů. Aplikace

je přenositelná mezi počítači pomoci USB flash disku a dostupné jsou verze offline a online. Podporuje operační systém Windows, Linux, Mac OS X, iOS, android, Windows Phone a SymbianOS. Hesla je vygenerovat podle jednoduchých pravidel. Uživatel si zvolí, jestli chce generovat speciální znaky, číslice, písmena a vyloučit podobné znaky. Databáze hesel je šifrovaná pomocí algoritmů AES, RC6, Blowfish. Nechybí podpora aplikací, více faktorová autentizace, bezpečnostní poznámky, virtuální klávesnice a automatické odhlášení. Aplikace umí import a export dat ve formátu CSV a HTML [27].

Sticky Password

Sticky password je aplikace od českých vývojářů. Řešení nabízí stejná jako Roboform. Tedy verzi free, professional, cloudová a podniková. Ve verzi free chybí možnost synchronizace mezi zařízeními, ukládání do cloudu a prioritní podpora. Verze professional stojí na rok 30 dolarů a doživotní licence 150 dolarů. Sticky Password podporuje automatické vyplňování formulářů, či aplikací a přenosnou verzi. Podporuje operační systém Windows, Mac OS X, iOS, Android. Generátor hesel je standardní s možností volby speciálních znaků, číslic, písmen a vyloučení podobných znaků. K dispozici je několik druhů šifrovacích algoritmů: AES, Twofish a Sapphire II. Databáze je přístupná, až po zadání hlavního hesla. Aplikaci lze sdílet s ostatními uživateli, aniž by se dostali k cizím heslům. Dalšími funkcemi jsou ukládání poznámek, více faktorová autentizace, virtuální klávesnice, automatické odhlášení a import/export souborů. Celkově je Sticky Password uživatelsky jednoduchá a flexibilní aplikace [28].

Dashlane

Dashlane je další z ověřených programů, pro ukládání hesel. Je dostupný ve verzi free a professional. Verze professional stojí 40 dolarů ročně a navíc od verze free umí zálohovat do cloudu, synchronizaci mezi zařízeními a přístup do aplikace přes webové rozhraní. Rozhraní je jednoduché na ovládání. Nechybí automatické vyplňování formulářů, podpora dvou faktorové autentizace a možnost sdílet hesla s vybranými kontakty v případě, že uživatel zapomene své přihlašovací heslo do aplikace. Podporován je operační systém Windows, OS X, Android, iOS, a doplňky pro Chrome, Firefox, Safari, a Internet Explorer. Dashlane umí měnit všechna hesla naráz pomocí

jednoho kliknutí a provádí audit hesel. Upozorní uživatele na slabá hesla, které je potřeba změnit. Není však možné nastavit generátor podle bezpečnostních politik. Program posílá upozornění, pokud je některý z uživatelských účtů napaden. Tato funkce funguje jen na webová hesla a program musí být online. Je použit šifrovací algoritmus AES. Dalšími funkcemi jsou ukládání poznámek, automatické odhlášení a import/export souborů ve formátech CSV a HTML [29].

KeePass

KeePass patří mezi známé správce hesel s rozsáhlou komunitou a je přeložen do více jak 30 světových jazyků. Program je zcela zdarma a je open source. Jedná se oblíbený program uživatele, kteří nechtějí ukládat svoje hesla v cloudu. Tento program nespolupracuje automaticky s webovým rozhraním a aplikacem. Podporuje operační systém Windows, Linux, Mac OS X, BSD. Jelikož se jedná o open source program, existuje velké množství doplňků jako například: virtuální klávesnice, další šifrovací algoritmy a offline sdílené mezi zařízeními. KeePass má velmi dobrý generátor hesel. Nechybí tak možnost volby speciálních znaků, číslic, písmen a vyloučení podobných znaků. Lze však nahrát i vlastní skripty pro generování hesel. Jako šifrovací algoritmus je použit AES a po stažení doplňků algoritmy Twofish, Serpent, GOST a další. Uživatelské rozhraní je standardní a velmi jednoduché, i když možnosti nastavení jsou opravdu veliké. V horní části je panelový nástroj. Vlevo jsou kategorie záznamů, které mají stromovou strukturu. Hesla se ukládají do různých databází, které se uživatel vytvoří. Export/import souborů lze provést do textového souboru, CSV, XML. V programu lze nastavit velké omezení akcí, což přispívá k vyšší bezpečnosti. Jedná se například o zákaz importu/exportu souborů, instalování doplňků apod. Dalšími funkcemi jsou automatické odhlášení při nečinnosti počítače, přenosná verze, více faktorová autentizace [30].

Password safe

Password Safe je jako Keepass open source a je zcela zdarma. Existuje však zpoplatněná verze, která umožňuje synchronizaci hesel mezi ostatními zařízeními. Přeložen je do 15 světových jazyků. Záznamy jsou řazeny do stromových struktur. Hesla se ukládají stejně jako u KeePass do databáze. Heslo do databáze je chráněna

hlavním heslem. Rozhraní programu působí zastarale, ale je plně funkční a intuitivní. Jako KeePass nespolupracuje s prohlížeči a aplikacemi. Oficiálně podporuje operační systém Windows. Upravená verze aplikace od jiných autorů podporuje další operační systémy na mobilních zařízeních a dále Linux, Mac OS X. Pro program existují doplňky, ale není jich tolik jako u KeePass. Generátor hesel má velké možnosti nastavení, chybí mu však generování hesel podle vlastních skriptů. Databáze hesel je šifrovaná algoritmem Twofish. Podporuje import/export souborů ve formátech XML, TXT, CSV. V programu lze nastavit politika hesel a celkově jsou možnosti nastavení na velmi dobré úrovni. Dalšími funkcemi jsou automatické odhlášení při nečinností počítače, přenosná verze a dvou faktorová autentizace [31].

2.6 Zhodnocení současného stavu

Identity management ve společnosti je na velmi pokročilé úrovni. Za silné stránky považuji proces recertifikace přístupů QEV a CBN. Podrobně zpracovanou dokumentaci procesů, pravidelný interní audit a kvalitní management rizik.

Společnost je silně byrokratická, čemuž odpovídají procesy a rozsáhlé směrnice. Postupnými akvizicemi a přizpůsobením se požadavkům zákazníka, považuji za slabou stránku heterogenitu nástrojů pro řízení identit. Existují případy, kdy mají problém s kompatibilitou. V nástrojích probíhají procesy automaticky, v některých však manuálně. Z tohoto hlediska by v tuto chvíli byla implementace jednotného přihlášení příliš složitá a nákladná. V příštích několika letech je strategie společnosti postupně celý IdM systém konsolidovat a staré nástroje nahrazovat novými.

Chybí postup bezpečného ukládání hesel, pokud si to situace vyžaduje. Při porušení bezpečnostní politiky závisí velikost postihu na managementu společnosti. Nastaly situace, kdy zaměstnanci sdíleli svůj osobní účet, což je závažný prohřešek porušení bezpečnosti.

Za hlavní nedostatek považuji absenci jednotného přihlášení. Jelikož uživatelé potřebují přístupu do několika desítek tisíc serverů, jsou na ně kladeny silné požadavky na pamatování hesel. Roste tak riziko ukládání hesel v nešifrované podobě, čímž dojde k porušení bezpečnostní politiky.

Slabinu vidím v procesu, kdy zaměstnanec přechází do jiného oddělení. Přechod je uskutečněn koncem každého měsíce, kdy také oddělení lidských zdrojů tuto skutečnosti kontroluje. Manažerům pak rozesílá email, aby zaměstnanci smazal přístupová práva. Podle směrnic musí být všechna oprávnění ze všech interních systémů odstraněna do čtrnácti dnů a ze systémů zákazníka do třech dnů. Pokud má uživatel administrátorská oprávnění, práva musí být odstraněna do třech dnů i v případě, že se jedná o interní systémy. Problém nastává v okamžiku, kdy email přehlédne nebo na povinnost smazat práva zapomene. Nehledě na to, že někdy musí tuto povinnost delegovat na další lidi a vzniká další časová prodleva. Zaměstnanec má potom přístupy, které nepotřebuje a dochází k porušení politik. Správné přidělení práv sice napraví kontrola CBN, která probíhá jedenkrát ročně.

Součástí analýzy také bylo zmapování trhu trezorů hesel. Jejich Analýza bude sloužit jako podklad při návrhu řešení.

3 NÁVRH ŘEŠENÍ

Při návrhu řešení budu vycházet z výsledků analýzy současného stavu a teoretických poznatků, které jsem načerpal z osobních konzultací, knižních a internetových zdrojů.

Je třeba navrhnout opatření pro:

- Bezpečné uložení hesel.
- Včasné přidělení a odebrání oprávnění zaměstnance, který přechází mezi odděleními.
- Sdílení jednoho účtu více uživateli.

3.1 Uložení hesel

Je potřeba navrhnout řešení k chybějícímu systému jednotného přihlášení. V některých případech zaměstnanci potřebují znát více hesel. Hrozí zde riziko, že je budou ukládat do nešifrovaných dokumentů v pracovních stanicích. Navrhuji proto zavést užívaní trezoru hesel. Uživatel si bude pamatovat pouze jedno přístupové heslo. Ostatní hesla si uživatel v trezoru uloží. Když se bude chtít přihlásit do některého ze systémů, heslo jednoduše zkopíruje. Výhodou je, že pro přístup ke všem heslům, postačí jen jedno přístupové.

Pro větší bezpečnost a zároveň splnění bezpečnostní politiky, lze však uvažovat pouze o lokálních trezorech. Dále musí být bezpodmínečně splněny tyto podmínky:

- Šifrovaná databáze hesel s délkou klíče 256bit.
- Program musí být kompatibilní se systémem Windows.
- Společnost neukončila svoji činnost a vydává aktualizace.
- Hesla nejsou při zadávání zobrazována.

V další kapitole budou na základě výše zmíněných požadavků porovnány trezory Roboform, Stiicky Password, Dashlane, Keepass a Password Safe. Na základě porovnání jejich funkcí a vlastností bude vybrán ten nejvhodnější. LastPass a Passpack

nesplnily požadavky, protože jsou pouze online. V úvahu připadají trezory pro individuální potřeby uživatele. Je zbytečné vybírat robustní řešení s centralizovanou databází pro všechny uživatele, které by bylo složité na integraci a finančně náročné.

3.1.3 Hodnocení programů

V následující tabulce je zobrazen a ohodnocen souhrn vlastností a funkcí trezorů hesel. Hodnotí se symbolem „✓“, maximální hodnocení je „✓✓✓✓“. Hodnotí se jen ty vlastnosti a funkce, které jsou stěžejní pro závěrečné doporučení implementace trezoru ve společnosti XYZ. Například sdílení hesel v cloudu je nepotřebná funkce. Verze zdarma se od placených liší v online přístupu, synchronizaci a ukládání do cloudu. Tyto funkce nejsou z hlediska návrhu doporučení důležité. Jediný Roboform free má omezení na počet uložených hesel. V tabulce jsou proto uvedeny jenom verze zdarma.

Tabulka 1: Hodnocení programů

	Roboform	Sticky Password	Dashlane	KeePass	Password Safe
Kompatibilita s operačními systémy	✓✓✓✓	✓✓✓	✓✓	✓✓✓	✓
Bezpečnostní politika	✓✓	✓✓	✓	✓✓✓✓	✓✓✓
Generátor hesel	✓✓	✓✓	✓	✓✓✓✓	✓✓✓
Síla šifrování databáze	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓	✓✓✓✓
Více faktorová autentizace	✓	✓	✓	✓	✓
Psaní poznámek	✓	✓	✓	✓	✓
Přenosná verze	✓	✓	x	✓	✓
Export/import	✓✓✓	✓✓	✓✓✓	✓✓✓✓	✓✓✓✓
Podpora aplikací	✓	✓	x	x	x
Vyplňování formulářů	✓	✓	✓	x	x
Množství uložených hesel	10	neomezeně	Neomezeně	neomezeně	Neomezeně
Uživatelské rozhraní	✓✓	✓✓✓	✓	✓✓✓	✓✓✓
Celkové hodnocení	✓	✓✓✓	✓	✓✓✓✓	✓✓✓

Zdroj: Vlastní zpracování

Jako vhodný program pro správu hesel navrhuji KeePass. Kromě podpory mobilních zařízení je podporován všemi operačními systémy. Má nejvíce možností nastavení, je přehledný a jednoduchý. Nejvíce podobný je mu Password Safe. Bohužel

podporuje pouze operační systém Windows, a proto byl upřednostněn KeePass. V úvahu připadal i Sticky Password. Ten je však více zaměřen online a má tendenci ukládat hesla do cloudu. Při prvním přihlášení si žádá zadat emailovou adresu. Pokud chce uživatel uložit heslo, které není součástí webu, musí pro uložení zadat neexistující webovou adresu, aby se heslo uložilo. KeePass na jednu stranu nepodporuje aplikace a ani vyplňování webových formulářů, na druhou stranu má široké možnosti nastavení, zdrojový kód může být podle potřeby upravován a uživatelské rozhraní je velice jednoduché na ovládání. Nutno podotknout, že existují doplňky, jež některé nedostatky odstraňují.

3.1.4 Implementace KeePass

Implementace bude probíhat následujícím způsobem:

1) Podá se žádost na začlenění mezi ostatní programy, které jsou součástí tzv. zelených stránek. Odtud mohou uživatelé stahovat software třetích stran pro pracovní účely.
2) KeePass bude prozkoumán a schválen kompetentním pracovníkem nebo týmem pracovníků, kteří jsou za tento výkon zodpovědní.
3) Vytvoří se uživatelský manuál. I když na oficiálních stránkách programu existuje průvodce, je komplexní a pro běžného uživatele je nepřehledný.
4) Uživatelům se pošle hromadný email, že mohou používat Keepass pro bezpečné uložení svých hesel.
5) Keepass se stane součástí povinného budování bezpečnostního povědomí. Uživatelé se o něm musí při školení dovědět.
6) Implementace bude zdokumentována.
7) Doplní se směrnice.

3.1.5 Návrh směrnic

Do směrnic je potřeba doplnit:

- Je zakázáno instalovat doplňky, které nejsou schváleny na zelených stránkách společnosti XYZ.
- Uživatel je povinen si vytvořit hlavní heslo do trezoru, které si zvolí nebo vygeneruje v souladu s politikou hesel.

- Ukládání hesel v pracovních stanicích jiným způsobem než za použití heslového trezoru je zakázáno. Pokud takový seznam hesel existuje, je potřeba provést import hesel do trezoru a starý seznam odstranit.
- Je povoleno používat přenosnou verzi heslového trezoru, avšak přenosné médium musí být šifrováno.

Další body, které se vztahují na KeePass jako na software třetí strany, jsou již součástí směrnic společnosti XYZ. Jedná se například o stahování povinných aktualizací, používání softwaru pouze k pracovním účelům atd.

3.2 Proces přechodu zaměstnanců

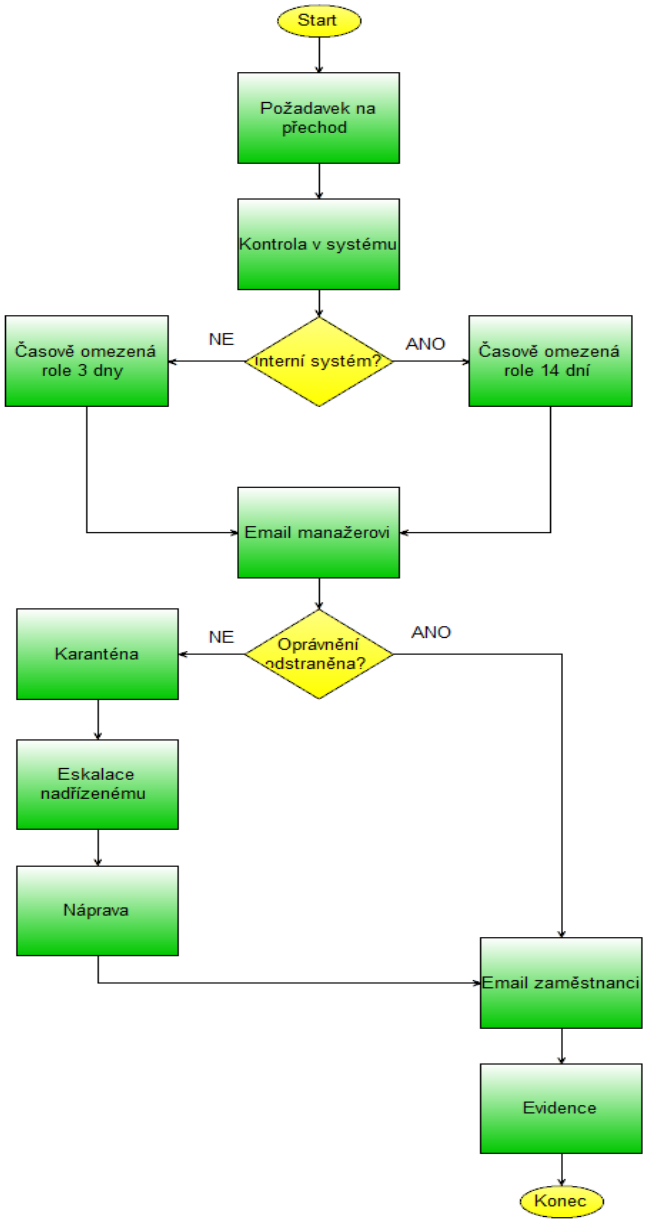
Včasné přidělení/odebrání přístupových zaměstnanců, kteří přechází mezi odděleními, lze řešit návrhem více opatřeními. Pro vylepšení celého procesu navrhuji zavést časově omezené role a eskalaci nadřízenému.

Časově omezená role bude mít tyto atributy:

- Jméno role
- Datum vytvoření
- Datum expirace
- Popis
- Typ role
- Schvalovatel
- Žadatel

O přidělení nebo odebrání role se postará úloha, která v HR systému prohledá všechny záznamy o identitách, jež mají naplánovaný přechod do jiného oddělení. Pokud bude potvrzená shoda, role se uživateli přiřadí. Časově omezená role zdědí vlastnosti původní role, jelikož role mají hierarchickou strukturu.

V následujícím obrázku je zobrazen celý proces přechodu zaměstnance s navrženými opatřeními.



Obr.č. 13: Proces přechodu zaměstnance

Zdroj: Vlastní zpracování

Proces začíná požadavkem na přechod, který zadá manažer zaměstnance. V systému lidských zdrojů se na konci každého měsíce kontroluje přechod

zaměstnance. Ověří se také, jestli se jedná o interní systémy společnosti nebo systémy zákazníka. Pro interní systémy se expirace časové role nastaví podle politik na 14 kalendářních dní od přechodu a v systémech zákazníka na 3 kalendářní dny. Manažer obdrží automaticky email, v kterém je upozorněn, na povinnost smazat přístupová prává zaměstnance do určitého data. V kompetenci manažera je úkol delegovat například na člena svého týmu. Pokud manažer přístupová práva odstraní, systém tuto událost detekuje a expirace role se nastaví na dobu neurčitou. Dále je zaměstnanci automaticky poslán informační email. Proces se automaticky zaeviduje a končí. Pokud manažer z nějakého důvodu přístupy nesmaže a časová role expiruje, proběhne deaktivace tzv. uložení role do karantény. Není možné ji upravovat, ale role je stále zachována. V dalším kroku provede automatické workflow eskalaci nadřízenému manažerovi, který svého podřízeného upozorní, aby přístupu odstranil. Nadřízený může provést nápravu sám, pokud má dostatečné kompetence a ví, které oprávnění je zaměstnanci potřeba odebrat. Oprávnění se odstraní, zaměstnanci je poslán email, proběhne evidence pro audit a proces končí.

Odstranit oprávnění nelze udělat automaticky, jelikož některé přístupy zaměstnanec nezbytně potřebuje pro vykonávání své práce. V případě ztráty přístupů přecházejících zaměstnanců nese manažer plnou zodpovědnost.

Problém může nastat, pokud se nejedná o plně automatický nástroj řízení identit. V tomto případě nelze zavést časově omezené role. Je potřeba se spoléhat především na lidský faktor. Pokud manažer odstraní přístupy, musí provést evidenci ručně. Například ve formě snímku obrazovky. HR systém by měl procházet někdo z kompetentního týmu, který má na starost řízení identit a po manažerovi si vyžádat důkaz o výkonu akce. To pouze v případě, pokud systém, ve kterém se odstranění oprávnění provádí, nedokáže synchronizovat data s HR systémem. Osoba, která si vyžádá důkaz o provedení akce, neprovádí recertifikaci role, ta je v kompetenci kontroly CBN.

3.2.1 Implementace opatření

1) Podání požadavku na zavedení jednotlivých opatření.
2) Po schválení se vytvoří časově omezené role.
3) Vytvoření úlohy, která bude kontrolovat systém a přiřadí zaměstnanci časově omezenou roli.

4) Vytvoření workflow pro eskalaci nadřízenému.
5) Určit zodpovědnou osobu pro kontrolu smazání oprávnění. Týká se manuálních nástrojů pro správu identit.
6) Obeznámení manažerů s novým procesem.
7) Celý proces zdokumentovat.
8) Vypracování směrnic.

3.2.2 Návrh směrnic

Pro nově navržená opatření je do směrnic potřeba doplnit:

- Manažer nese plnou zodpovědnost v případě ztráty oprávnění zaměstnance.
- Nadřízený manažer je povinen podřízeného informovat o nápravě, v případě potřeby provede nápravu on sám.
- Pokud nástroj pro řízení identit nesynchronizuje data s HR systémem, musí být manažer vyzván kompetentní osobou pro předložení důkazu o smazání oprávnění zaměstnance.
- Příslušná osoba, jež provádí kontrolu expiraci rolí, je povinna žádat od manažera důkaz o provedení akce. Pokud manažer důkaz nepředloží, je kontaktován jeho nadřízený. Týká se manuálních nástrojů pro správu identit.

3.3 Sdílení uživatelského účtu

Problém sdílení účtu s více uživateli je závažné porušení bezpečností politiky. Bohužel tomuto problému nelze zabránit technickým opatřením. Společnost má propracovaný systém budování bezpečnostního povědomí. Na druhou stranu uživatelé musí naráz vstřebat velké množství informací, co se bezpečnosti týče. Navrhuji proto do systému budování bezpečnostního povědomí zařadit reálné simulace a důsledky sdílení přístupových oprávnění. Při porušení navrhuji okamžité snížení pracovního ohodnocení a podstoupení disciplinárního řízení. Tyto kroky budou sloužit jako odstrašující příklad. Je potřeba zaměstnancům důsledně zdůraznit, že porušením sdílení přístupů jim hrozí vážný postih. Jestliže uživatel sdílel účet s někým jiným, společnost odhalí pomocí auditních záznamů. Pomocí nich lze sledovat přihlášení z neobvyklých míst v neobvyklém čase a vzniká tím podezření, že zaměstnanec heslo sdílel. Pro detekci

sdílení přístupových oprávnění společnosti navrhuji zavedení systému, který bude sledovat a vyhodnocovat podezřelé aktivy a potom jej integrovat se systémem IdM a Management bezpečnostních informací a událostí (SIEM).

3.4 Ekonomické zhodnocení

K implementaci opatření společnost nepotřebuje najímat žádné externí zaměstnance. Není potřeba pořizovat žádné licence. Dále není potřeba kompletně vypracovávat nové směrnice, jen je doplnit o určité body. Mezi nejvíce nákladové položky patří čas, který si vyžádá plnění procesu přechodu zaměstnance. Jedná se o vytvoření workflow, výkon osoby kontrolující role v HR systému a také aktivita nadřízeného manažera. Ten bude muset se svým podřízeným řešit situaci, když nedojde k odstranění oprávnění. Po schválení by implementace jednotlivých opatření měla zabrat několik hodin. Vzhledem k tržbám společnosti jsou náklady zanedbatelné. Opatření sníží pravděpodobnost výskytu bezpečnostních incidentů, což může v budoucnu ušetřit náklady.

ZÁVĚR

Cílem diplomové práce bylo navrhnout zlepšení pro systém řízení identit. Na základě analýzy současného stavu byla navržena opatření, která mají IdM zlepšit. Zavedením trezoru hesel se dosáhne vyšší bezpečnosti za přiměřeného uživatelského komfortu. Návrh opatření pro proces přechodu zaměstnanců zlepší dodržování politik. Na základě toho může společnost garantovat odebrání přístupů v SLA se zákazníkem. U tohoto opatření by bylo dobré zvážit, zda provádět recertifikaci přístupů častěji než jedenkrát ročně v případě manuálních nástrojů identit. Zajistí se tím, že zaměstnanci budou mít taková oprávnění, které skutečně potřebují. Avšak na úkor vyšších nákladů. Zavedení sankcí u sdílení účtů je bohužel jediné možné východisko vzhledem ke kvalitnímu systému budování bezpečnostního povědomí.

Celkově je IdM ve společnosti na vysoké úrovni. Slabinou je však heterogenita nástrojů. Pokud by všechny nástroje byly plně automatizované, mělo by to velký vliv na redukci nákladů a zvýšení bezpečnosti snížením zásahů lidského faktoru. Společnosti proto doporučuji provést co nejdříve postupnou konsolidaci. Bude pak mnohem jednodušší a levnější zavedení systému jednotného přihlášení.

LITERATURA

[1] ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: CERM, 2013. ISBN 978-80-7204-872-4.

[2] NOVÁK, L. a J. POŽÁR. Systém řízení informační bezpečnosti. *CyberSecurity.cz* [online]. [cit. 2015-12-29]. Dostupné z: www.cybersecurity.cz/data/SRIB.pdf

[3] POŽÁR J. *Základy teorie informační bezpečnosti*. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

[4] BŘICHÁČEK Z. Systém řízení bezpečnosti informací. *Blog.brichacek.net* [online]. [cit. 2015-12-30]. Dostupné z: http://blog.brichacek.net/audit-informacni- bezpecnosti-system-rizeni-informacni-bezpecnosti-isms/

[5] ČSN ISO/IEC 27000. *Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Přehled a slovník*. Praha: Český normalizační institut, 2014.

[6] ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Požadavky*. Praha: Český normalizační institut, 2013.

[7] ČSN ISO/IEC 27002. Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací. Praha: Český normalizační institut, 2013.

[8] BERTINO, E. a K. TAKAHASHI. *Identity management: Concepts, Technologies, and Systems*. Boston: Artech House, 2011. ISBN 978-1- 608807-039-8.

[9] JØSANG, A. a S. POPE. User Centric Identity Management. In: *AusCERT Asia Pacific Information Technology Security Conference.*[cit. 2016-1-17]. Dostupné

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.1563&rep=rep1&type=pdf

[10] LÍZNER M. Identity management – centrální správa uživatelských účtů. *Computerworld.cz* [online]. [cit. 2016-1-18]. Dostupné z: http://computerworld.cz/securityworld/identity-management-centralni-sprava-uzivatelskych-uctu-47568

[11] WATERS K.J a P. KHUDHUR. Abeceda identity MANAGEMENTU. *Businessworld.cz* [online]. [cit. 2016-1-18]. Dostupné z: http://businessworld.cz/bezpecnost-a-rizeni-rizik/abeceda-identity-managementu-1390

[12] SEMANČÍK R. Cesta k efektivnímu identity managementu**.** *Systemonline.cz* [online]. [cit. 2016-1-18]. Dostupné z: http://www.systemonline.cz/sprava-it/cesta-k-efektivnimu-idm-architektura-iam-reseni.htm

[13] A. PFITZMANN a M. HANSEN. A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. *PRIVACY AND DATA SECURITY* [online]. [cit. 2016-1-19]. Dostupné z: https://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[14] ITU. *ITU-T Recommendation Y.2720 - NGN identity management framework*. Geneva: International Telecommunication Union, 2009.

[15] SEMANČÍK, R a K. VALALIKOVÁ . Cesta k efektivnímu identity managementu**.** *Systemonline.cz* [online]. [cit. 2016-1-27]. Dostupné z: http://www.systemonline.cz/it-security/cesta-k-efektivnimu-identity-managementu.htm

[16] YIP D., G. WILLIAMSON, I. SHARONI a K. SPAULDING. *Identity Management: A Primer*. Lewisville: MC Press, 2009. ISBN 978-1583470930

[17] LÍZNER M. Identity management zjednodušuje správu uživatelských účtů. *Computerworld.cz* [online]. [cit. 2016-1-28]. Dostupné z: http://computerworld.cz/securityworld/identity-management-zjednodusuje-spravu-uzivatelskych-uctu-3-47977

[18] OSMANOGLU E. *Identity and Acess Management: Business Performance Through Connected Intelligence.* Waltham: Elsevier Science, Syngress, 2013. ISBN 978-0124104334.

[19] FERRAILO D. A D. KUHN. Role-Based Access Controls. In: *Baltimore 15th National Computer Security Conference*.[cit. 2016-1-28]. Dostupné z: http://arxiv.org/ftp/arxiv/papers/0903/0903.2171.pdf

[20] SEMANČÍK R. Cesta k efektivnímu identity managementu**.** *Systemonline.cz* [online]. [cit. 2016-1-29]. Dostupné z: http://www.systemonline.cz/sprava-it/cesta-k-efektivnimu-identity-managementu-2-dil.htm

[21] NORIS I. Cesta k efektivnímu identity managementu**.** *Systemonline.cz* [online]. [cit. 2016-1-29]. Dostupné z: http://www.systemonline.cz/sprava-it/cesta-k-efektivnimu-idm-provisioning.htm

[22] Powell J. *SCS Basic Education V2.1*. Prezentace. 2003.

[23] LAHUČKÝ, J. Kreativita, inovace a organizační kultura. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2012. 102 s. Vedoucí diplomové práce PhDr. Emilie Franková, Ph.D.

[24] RUBENKING NEIL. The Best Free Password Managers for 2016. *www.pcmag.com* [online]. [cit. 2016-5-9]. Dostupné z: http://www.pcmag.com/article2/0,2817,2475964,00.asp

[25] LASTPASS. LastPass SIMPLY YOUR LIFE. *lastpass.com* [online]. [cit. 2016-5-10]. Dostupné z: https://lastpass.com/cs/

[26] PASSPACK. PASSPACK Password Manager Secure. *Passpack.com* [online]. [cit. 2016-5-10]. Dostupné z: https://www.passpack.com/

[27] ROBOFORM. Make Your Life Easier with the Top Rated Password Manager. *Roboform.com* [online]. [cit. 2016-5-5]. Dostupné z: http://www.roboform.com/

[28] STICKY PASSWORD. Reviewer Guide – Core Functionality. *Sticky Password.com* [online]. [cit.2016-5-6]. Dostupné z: https://www.stickypassword.com/downloads/SP_Guide_v01_ENG.pdf

[29] DASH LANE. Dashlane help. *Dashlane.com* [online]. [cit. 2016-5-6]. Dostupné z: https://support.dashlane.com/hc/en-us

[30] KEEPASS. KeePass Password Safe. *KeePass.info* [online]. [cit. 2016-5-7]. Dostupné z: http://KeePass.info/

[31] PASSWORD SAFE. Password Safe Simple & Secure Password Management. *Pwsafe.org* [online]. [cit. 2016-5-7]. Dostupné z: https://pwsafe.org/index.shtml

SEAZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM TABULEK